

MACHINE-ASSISTED TRANSLATION (MAT):

(19) 【発行国】 日本国特許庁 (J P)	(19)[ISSUING COUNTRY] Japan Patent Office (JP)
(12) 【公報種別】 公開特許公報 (A)	(12)[GAZETTE CATEGORY] Laid-open Kokai Patent (A)
(11) 【公開番号】 特 開 2000-216774(P2000-216774A)	(11)[KOKAI NUMBER] Unexamined Japanese Patent 2000-216774(P2000-216774A)
(43) 【公開日】 平成 1 2 年 8 月 4 日 (2 0 0 0 . 8 . 4)	(43)[DATE OF FIRST PUBLICATION] August 4, Heisei 12 (2000. 8.4)
(54) 【発明の名称】 暗号文検証方法、そのプログラ ム記録媒体、及びその装置	(54)[TITLE OF THE INVENTION] The cryptogram verification method, its program recording medium, and its apparatus
(51) 【国際特許分類第 7 版】 H04L 9/32 G09C 1/00 640	(51)[IPC INT. CL. 7] H04L 9/32 G09C 1/00 640
【 F I 】 H04L 9/00 675 D G09C 1/00 640 C	[FI] H04L 9/00 675 D G09C 1/00 640 C
【審査請求】 未請求	[REQUEST FOR EXAMINATION] No
【請求項の数】 3 3	[NUMBER OF CLAIMS] 33
【出願形態】 O L	[FORM OF APPLICATION] Electronic

【全頁数】 21

[NUMBER OF PAGES] 21

(21) 【出願番号】

(21)[APPLICATION NUMBER]

特願平 11-15409

Japanese Patent Application Heisei 11-15409

(22) 【出願日】

(22)[DATE OF FILING]

平成 11 年 1 月 25 日 (1999
9. 1. 25)

January 25, Heisei 11 (1999. 1.25)

(71) 【出願人】

(71)[PATENTEE/ASSIGNEE]

【識別番号】

[ID CODE]

000004226

000004226

【氏名又は名称】

[NAME OR APPELLATION]

日本電信電話株式会社

Nippon Telegraph and Telephone CORP.

【住所又は居所】

[ADDRESS OR DOMICILE]

(72) 【発明者】

(72)[INVENTOR]

【氏名】

[NAME OR APPELLATION]

阿部 正幸

Abe Masayuki

【住所又は居所】

[ADDRESS OR DOMICILE]

(74) 【代理人】

(74)[AGENT]

【識別番号】

[ID CODE]

100066153

100066153

【弁理士】

[PATENT ATTORNEY]

【氏名又は名称】

[NAME OR APPELLATION]

草野 卓 (外 1 名)

Kusano Takashi (and 1 other)

【テーマコード (参考)】

[THEME CODE (REFERENCE)]

5J104

5J104

【F ターム (参考)】

[F TERM (REFERENCE)]

5J104 AA01 AA08 JA23 JA29
LA00 LA03 LA05 LA06 NA02
NA08 NA12 NA18

5J104 AA01 AA08 JA23 JA29 LA00 LA03 LA05
LA06 NA02 NA08 NA12 NA18

(57) 【要約】

(57)[ABSTRACT OF THE DISCLOSURE]

【課題】

[SUBJECT OF THE INVENTION]

検証式における値に関する情報を漏らすことなく、暗号文の正当性の有無を示すことができる。

The existence of the correctness of a cryptogram can be shown without leaking the information about the value in a verification type.

【解決手段】

[PROBLEM TO BE SOLVED]

p は大きな素数、 q は $p-1$ を割り切る大きな素数とし、 G_q の元 g_1, g_2 を任意に選択し、 $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $Z = g_1^z \bmod p$ を暗号化に用いる公開鍵とし、 $(x_1, x_2, y_1, y_2, z) \in \mathbb{Z}_q^5$ を秘密鍵とし、平文 m の暗号文 $E = (u_1, u_2, v, e)$ を受信し (S1)、乱数 r を生成し (S2)、 $c = H(u_1, u_2)$, $V = (u_1^{x_1 + cy_1} u_2^{x_2 + cy_2} v^{-1})^r \bmod p$ を計算し (S3)、 $V = 1$ なら暗号文を合格として復号し、不合格なら零知識証明により、 $r, x_1,$

It considers it as the big prime number among which p gives a clear-cut solution to a big prime number, and q gives $p-1$, and chooses the origin g_1 and g_2 of G_q as desired, let $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $Z = g_1^z \bmod p$ be the public key which it uses for encryption, let $(x_1, x_2, y_1, y_2, z) \in \mathbb{Z}_q^5$ be a secret key, it receives cryptogram $E = (u_1, u_2, v, e)$ of Plaintext m .

(S1), it forms a random number r .

(S2), $c = H(u_1, u_2)$, $v =$ (calculating $u_1^{x_1 + cy_1} u_2^{x_2 + cy_2} v^{-1})^r \bmod p$)

(S3), if it is $V = 1$, it decodes a cryptogram as a pass, if it is a rejection, it proves that it is a rejection by zero knowledge proof, without leaking a function secret to $r, x_1, x_2, y_1,$ and y_2 .

x_2 , y_1 , y_2 に関数秘密を漏らさずに不合格であることを証明する。

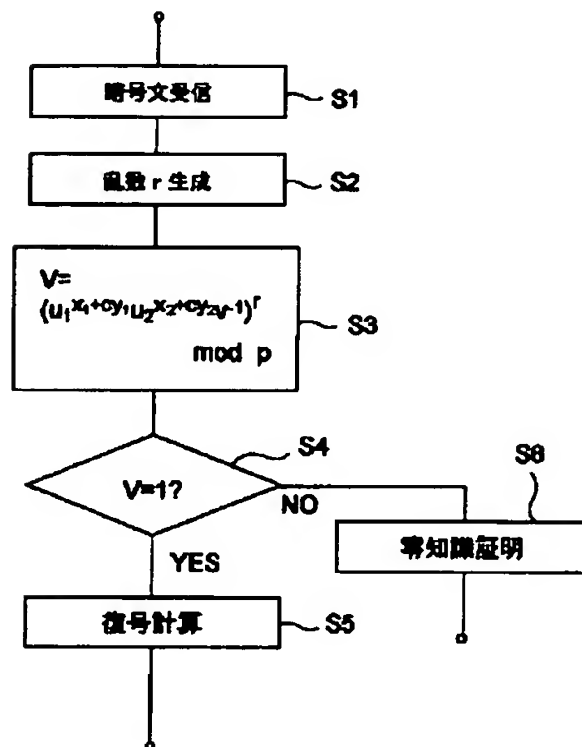


図 2

- S1 Cryptogram reception
 S2 Random-number r generation

 S5 Decoding calculation
 S6 Zero knowledge proof

【特許請求の範囲】

[CLAIMS]

【請求項 1】

[CLAIM 1]

受信した暗号文が正当に作られたものであることを、検証式の値が 1 になることを確認することによって検証する暗号文検証方法において、
 乱数 r を生成し、本来の検証式

A cryptogram verification method, in which in the cryptogram verification method which it verifies by checking that the cryptogram which received is made justly, and that the value of a verification type is set to 1, it forms a random number r , it verifies a cryptogram by checking

の値 V を r 乗した値が 1 になるか否かを確認することによって暗号文を検証することを特徴とする暗号文検証方法。

【請求項 2】

p を大きな素数、 q を $p-1$ を割り切る大きな素数とし、 G_q は乗法群 Z_{p^*} の位数 q の部分群を表すものとし、 g_1, g_2 は、 g_1 を底とする g_2 の離散対数が未知である G_q の元とし、 H を汎用ハッシュ関数とし、 $(x_1, x_2, y_1, y_2, z) \in Z_q^5$ を秘密鍵、 $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $Z = g_1^z \bmod p$ なる (X, Y, Z) を公開鍵とし、平文 m に対する暗号文 E は c を $H(u_1, u_2) \bmod q$ として $u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $v = X^r Y^{cr} \bmod p$ なる三つ組み (u_1, u_2, v) を含む暗号方法において、復号者装置は、乱数 r を生成し、 $c = H(u_1, u_2) \bmod q$ を計算し、

$V = (u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$ を計算し、 V が 1 に等しいことを確認することによって暗号文の正当性を検証することを特徴とする暗号文検証方法。

【請求項 3】

請求項 2 の暗号文検証方法に

whether the value which squared the value V of an original verification type r is set to 1.

[CLAIM 2]

A cryptogram verification method, in which considering it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to $p-1$, G_q shall express the partial group of the digit q of multiplicative-group Z_{p^*} .

G_1 and g_2 carry out g_1 the origin of G_q with a discrete unknown logarithm of g_2 which it uses as a bottom, let H be a general purpose hash function, it is a secret key about (x_1, x_2, y_1, y_2, z) (element of) Z_q^5 , $x = g_1^{x_1} g_2^{x_2} \bmod p$, $y = g_1^{y_1} g_2^{y_2} \bmod p$

Let $Z = g_1^z \bmod p$ be public key (X, Y, Z) , the cryptogram E with respect to Plaintext m

C , as $H(u_1, u_2) \bmod q$

Becomes $u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, and $v = X^r Y^{cr} \bmod p$.

In the cryptographic method containing 3 sets (u_1, u_2, v) , a decoding person apparatus forms a random number r , it calculates $c = H(u_1, u_2) \bmod q$,

$V = (\text{calculating } u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$

It verifies the correctness of a cryptogram, when V checks that it is equal to 1.

[CLAIM 3]

In the cryptogram verification method of Claim

において、 V が1に等しくない場合に、

零知識証明を用いて第三者に V がある乱数 r に対して $(u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$ のように計算した結果であることを証明することを特徴とする暗号文検証方法。

2, when V is not equal to 1, to the random number r which has V to a third person using zero knowledge proof (it proves that it is the result of calculating like $u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$.)

The cryptogram verification method characterized by the above-mentioned.

【請求項4】

p を大きな素数、 q を $p-1$ を割り切る大きな素数とし、 G_q は乗法群 Z_p の位数 q の部分群を表すものとし、 g_1, g_2 を G_q の元とし、 H を汎用ハッシュ関数とし、

n 人の復号者を $P_1 \sim P_n$ とし、各復号者 P_j は固有の公開値 w_j を持ち、

$(x_1, x_2, y_1, y_2, z) \in Z_q^5$ を $3 \leq t < n$ を満たすしきい値 t の秘密分散法により分散して得られる、値 w_j に対応する秘密値 $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ を復号者 P_j の秘密鍵とし、

$X_j = g_1^{x_{1j}} g_2^{x_{2j}} \bmod p$,
 $Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p$,
 $Z_j = g_1^{z_j} \bmod p$ なる (X_j, Y_j, Z_j) を復号者 P_j の公開鍵とし、

各々の復号者装置間には、安全な通信路があるものとし、また、各復号者装置は、他の全員の復号者装置が同一の内容を受信す

[CLAIM 4]

A cryptogram verification method, which considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to $p-1$, G_q shall express the partial group of the digit q of multiplicative group Z_p .

It carries out g_1 and g_2 the origin of G_q , let H be a general purpose hash function, it sets n persons' decoding person to P_1-P_n , each decoding person P_j has the inherent open value w_j , (x_1, x_2, y_1, y_2, z)

Let the secret value $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ corresponding to a value w_j acquired by dispersing (element of) Z_q^5 with the secret dispersion method of threshold-value t which fills $3 \leq t < n$ be the decoding person's P_j secret key, let $X_j = g_1^{x_{1j}} g_2^{x_{2j}} \bmod p$, $Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p$, and $Z_j = g_1^{z_j} \bmod p$ be the decoding person's P_j public key (X_j, Y_j, Z_j) ,

A safe communication channel shall be between each decoding person apparatus.

Moreover, that each decoding person apparatus receives the content with all the members' same

ることが保証される放送型通信路を利用できるものとし、乱数 $r \in Z_q$ をしきい値 t の秘密分散法により分散して得られる、値 w_j に対応する秘密値 r_j を復号者 P_j は保持するものとし、

$E = (u_1, u_2, v, e)$ を、 $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $Z = g_1^z \bmod p$ を公開鍵とした平文 m の暗号文とし、正しい暗号文は $u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $c = H(u_1, u_2)$, $v = X^r Y^{cr} \bmod p$, $e = m Z^r \bmod p$ を満足するとき、 E を受信した各復号者 P_j の装置は、 $c = H(u_1, u_2)$ を計算し、

$V_j = (u_1^{x_1 + cy_1} u_2^{x_2 + cy_2} v^{-1})^{r_j} \bmod p$ を計算し、

V_j をしきい値 t 以上 $2t$ 以下の検証可能秘密分散法により分散して得られる、値 w_k に対応する秘密値 V_{jk} を各復号者 P_k の装置に安全な通信路を介して送信し、

他の全ての復号者装置から V_{jk} を受信した復号者 P_k の装置は、放送型通信路により、 V_k を他の全ての復号者装置へ送信し、

V_k を受信した各復号者 P_j の装置は対応する V_{kj} を放送型通信路により他の全ての復号者

other decoding person apparatus shall utilize the broadcast type communication channel guaranteed.

The decoding person P_j shall maintain the secret value r_j corresponding to a value w_j acquired by dispersing random-number r (element of) Z_q with the secret dispersion method of threshold-value t .

Let $E = (u_1, u_2, v, e)$ be the cryptogram of plaintext m which used $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, and $Z = g_1^z \bmod p$ as public key, when the correct cryptogram satisfies $u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $c = H(u_1, u_2)$, $v = X^r Y^{cr} \bmod p$, and $e = m Z^r \bmod p$, the apparatus of each decoding person P_j who received E calculates $c = H(u_1, u_2)$,

$V_j = (\text{calculating } u_1^{x_1 + cy_1} u_2^{x_2 + cy_2} v^{-1})^{r_j} \bmod p)$

It transmits the secret value V_{jk} corresponding to a value w_k acquired by dispersing V_j with t or more threshold values and a verifiable secret dispersion method $2t$ or less through a communication channel safe for each decoding person's P_k apparatus, the apparatus of the decoding person P_k who received V_{jk} from all other decoding person apparatus transmits V_k to all other decoding person apparatus according to a broadcast type communication channel, the apparatus of each decoding person P_j who received V_k transmits corresponding V_{kj} to all other decoding person apparatus according to a broadcast type communication channel, it verifies that each

装置へ送信し、各復号者装置は各 V_k が正しい値であることを受信した全ての V_{kj} を用いて検証し、

正しいと確認された V_k のうち $2t+1$ 個を選択し、指数部に対する秘密復元手順により復元した値 V が 1 に等しいか否かを調べ、等しくないならば他の $2t+1$ 個の組み合わせで同様に秘密復元手順を繰り返し、全ての組み合わせについていずれも復元値が 1 に等しくないならば、その暗号文を不正と判定し、一つでも 1 になる組み合わせがあったならば、その暗号文を正しいと判定することを特徴とする暗号文検証方法。

【請求項 5】

請求項 4 の暗号文検証方法において、
上記暗号文が正しいと判定され
ると、
 w を $\text{mod } q$ での 1 の n 乗根とし、各復号者装置は、 w_j を $w^{j-1} \text{mod } q$ とし、 $1 < j < n$ において $w_j \neq 1$ を満たすような w_j を公開の固有値とし、
各復号者 P_j の装置は $D_j = u \cdot 1^{z_j} \text{mod } p$ を計算し、放送型通信路により他の全ての復号者装置へ送信し、受信した (D_1, \dots, D_n) の u を底とする離散対数が BCH 符号のコードワ

decoding person apparatus is each value with correct V_k using all $V_{kj}(s)$ that received,

If correct, it will choose $2t+1$ piece among checked $V_k(s)$, it examines whether the value V decompressed with the secret decompression procedure with respect to an index part is equal to 1, if not equal, it repeats a secret decompression procedure similarly in other $2t+1$ piece combination, about all combination, if the decompression value is not all equal to 1, it will judge that the cryptogram is irregular, if there is combination set to 1 at least one, it will judge that the cryptogram is correct.

[CLAIM 5]

A cryptogram verification method, in which in the cryptogram verification method of Claim 4, if judged with the above-mentioned cryptogram being correct, let w be n root of 1 in $\text{mod } q$, each decoding person apparatus makes $w_j = w^{j-1} \text{mod } q$, it considers it as the eigenvalue of public presentation of w_j which fills $w_j \neq 1$ in $1 < j < n$, each decoding person's P_j apparatus calculates $D_j = u \cdot 1^{z_j} \text{mod } p$, it transmits to all other decoding person apparatus according to a broadcast type communication channel, it checks that the discrete logarithm which uses as a bottom u which received (D_1, \dots, D_n) is the coding word of a BCH code.

ードであることを確認すること、を特徴とする暗号文検証方法。

【請求項 6】

p を大きな素数、 q を $p-1$ を割り切る大きな素数とし、 G_q は乗法群 Z_{p^*} の位数 q の部分群を表すものとし、 g_1 , g_2 は、 g_1 を底とする g_2 の離散対数が未知である G_q の元とし、 H を汎用ハッシュ関数とし、 $(x_1, x_2, y_1, y_2, z) \in Z_{q^5}$ を秘密鍵、 $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $Z = g_1^z \bmod p$ なる (X, Y, Z) を公開鍵とし、平文 m に対する暗号文 E は c を $H(u_1, u_2) \bmod q$ として $u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $v = X^r Y^{\alpha} \bmod p$ なる三つ組み (u_1, u_2, v) を含む暗号方法において、復号者装置は、乱数 r を生成し、 $x_1' = x_1 \cdot r \bmod q$, $x_2' = x_2 \cdot r \bmod q$, $y_1' = y_1 \cdot r \bmod q$, $y_2' = y_2 \cdot r \bmod q$ を計算し、

受信した暗号文から、 $c = H(u_1, u_2) \bmod q$ を計算し、 $V = u_1^{x_1' + cy_1'} u_2^{x_2' + cy_2'} v^{-r} \bmod p$ を計算し、 V が 1 に等しいことを確認することによって暗号文の正当性を検証することを特徴とする暗号文検証方法。

[CLAIM 6]

A cryptogram verification method, which considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to $p-1$, g_1, g_2 shall express the partial group of the digit q of multiplicative-group Z_{p^*} .

G_1 and g_2 carry out g_1 the origin of G_q with a discrete unknown logarithm of g_2 which it uses as a bottom, let H be a general purpose hash function, (x_1, x_2, y_1, y_2, z)

Let a secret key, $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, and $Z = g_1^z \bmod p$ be public key for (element of) Z_{q^5} (X, Y, Z) , the cryptogram E with respect to Plaintext m

Making c into $H(u_1, u_2) \bmod q$.

$U_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, it becomes $v = X^r Y^{\alpha} \bmod p$.

In the cryptographic method containing 3 sets (u_1, u_2, v) , a decoding person apparatus forms a random number r , it calculates $x_1' = x_1$ and $r \bmod q$, $x_2' = x_2$ and $r \bmod q$, $y_1' = y_1$ and $r \bmod q$, and $y_2' = y_2$ and $r \bmod q$,

From the cryptogram which received, it calculates $c = H(u_1, u_2) \bmod q$, it calculates $V = u_1^{x_1' + cy_1'} u_2^{x_2' + cy_2'} v^{-r} \bmod p$, it verifies the correctness of a cryptogram, when V checks that it is equal to 1.

【請求項 7】

請求項 6 の暗号文検証方法において、
 V が 1 に等しくない場合に、復号者装置は (X, Y, V) が、ある (x_1, x_2, y_1, y_2, r) に対して $X = g^{x_1} g^{x_2} \text{mod } p$, $Y = g^{y_1} g^{y_2} \text{mod } p$, $V = u^{x_1 r + y_1 r} u^{x_2 r + y_2 r} v^{-r} \text{mod } p$ を満足することを零知識証明を用いて (x_1, x_2, y_1, y_2) を秘密としたまま検証者に証明することを特徴とする暗号文検証方法。

[CLAIM 7]

A cryptogram verification method, in which in the cryptogram verification method of Claim 6, when V is not equal to 1, as for a decoding person apparatus, (X, Y, V) , receive that it is (x_1, x_2, y_1, y_2, r) .

It zero-knowledge-proves satisfying $X = g^{x_1} g^{x_2} \text{mod } p$, $Y = g^{y_1} g^{y_2} \text{mod } p$, $V = u^{x_1 r + y_1 r} u^{x_2 r + y_2 r} v^{-r} \text{mod } p$.

Using this, it proves to a verification person, making secret (x_1, x_2, y_1, y_2) .

【請求項 8】

請求項 7 の暗号文検証方法において、
 g, h は g を底とする h の離散対数が未知であるような G_q の元であって、
 復号者装置は、乱数 r, a_1, a_2, b_1, b_2 を生成し、
 $R = g^r h^a \text{mod } p$, $RX_1 = R^{x_1} h^{a_1} \text{mod } p$, $RX_2 = R^{x_2} h^{a_2} \text{mod } p$, $RY_1 = R^{y_1} h^{b_1} \text{mod } p$, $RY_2 = R^{y_2} h^{b_2} \text{mod } p$ なる $R, RX_1, RX_2, RY_1, RY_2$ を公開し、

[CLAIM 8]

A cryptogram verification method, in which in the cryptogram verification method of Claim 7, g and h are under G_q whose discrete logarithm of h which uses g as a bottom is unknown, comprised such that a decoding person apparatus forms random numbers r, a_1, a_2, b_1 , and b_2 , it exhibits $R, RX_1, RX_2, RY_1, RY_2$ used as $R = g^r h^a \text{mod } p$, $RX_1 = R^{x_1} h^{a_1} \text{mod } p$, $RX_2 = R^{x_2} h^{a_2} \text{mod } p$, $RY_1 = R^{y_1} h^{b_1} \text{mod } p$, $RY_2 = R^{y_2} h^{b_2} \text{mod } p$,

$(X, Y, V, R, RX_1, RX_2, RY_1, RY_2)$ がある
 $(x_1, x_2, y_1, y_2, r, a_1, a_2, b_1, b_2)$ に対して、 $X = g^{x_1} g^{x_2} \text{mod } p$, $Y = g^{y_1} g^{y_2} \text{mod } p$, $V = u^{x_1 r + y_1 r} u^{x_2 r + y_2 r} v^{-r} \text{mod } p$, $r = g^r h^a \text{mod } p$, $RX_1 = R^{x_1} h^{a_1} \text{mod } p$, $RX_2 = R^{x_2} h^{a_2} \text{mod } p$, $RY_1 = R^{y_1} h^{b_1} \text{mod } p$, $RY_2 = R^{y_2} h^{b_2} \text{mod } p$,

To $(x_1, x_2, y_1, y_2, r, a_1, a_2, b_1, b_2)$ with $(X, Y, V, R, RX_1, RX_2, RY_1, RY_2)$, $x = g^{x_1} g^{x_2} \text{mod } p$, $y = g^{y_1} g^{y_2} \text{mod } p$, $v = u^{x_1 r + y_1 r} u^{x_2 r + y_2 r} v^{-r} \text{mod } p$, $r = g^r h^a \text{mod } p$, $RX_1 = R^{x_1} h^{a_1} \text{mod } p$, $RX_2 = R^{x_2} h^{a_2} \text{mod } p$, $RY_1 = R^{y_1} h^{b_1} \text{mod } p$, $RY_2 = R^{y_2} h^{b_2} \text{mod } p$,

p , $Y = g_1^{y_1} g_2^{y_2} \bmod p$,
 $V = u_1^{x_1 r + c y_1 r} u_2^{x_2 r + c y_2 r}$
 $v^{-r} \bmod p$, $R = g^r h^a \bmod p$,
 $R X_1 = R^{x_1} h^{a_1} \bmod p$,
 $R X_2 = R^{x_2} h^{a_2} \bmod p$, $R Y_1 = R^{y_1} h^{b_1} \bmod p$, $R Y_2 = R^{y_2} h^{b_2} \bmod p$ なる関係式を満たすことを零知識証明によって証明することを特徴とする暗号文検証方法。

$$R Y_2 = R^{y_2} h^{b_2} \bmod p$$

It proves filling the relation used as this by zero knowledge proof.

【請求項 9】

請求項 6 の暗号文検証方法において、
 n 人の復号者を $P_1 \sim P_n$ とし、
 w を $\bmod q$ での 1 の n 乗根とし、
 w_j を $w^{j-1} \bmod q$ とし、 $1 < j < n$ において $w_j \neq 1$ を満たすものとし、各復号者 P_j に値 w_j を割り当て、
 復号者 P_j の秘密鍵 $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ は、 $3 \leq t < n$ を満たすしきい値 t の秘密分散法により (x_1, x_2, y_1, y_2, z) を分散して得られる、値 w_j に対応する秘密値とし、

$X_j = g_1^{x_{1j}} g_2^{x_{2j}} \bmod p$,
 $Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p$,
 $Z_j = g_1^{z_j} \bmod p$ なる (X_j, Y_j, Z_j) を復号者 P_j の公開鍵とし、

各々の復号者装置間には、安全な通信路があるものとし、また、

[CLAIM 9]

A cryptogram verification method, in which in the cryptogram verification method of Claim 6, it sets n persons' decoding person to $P_1 \sim P_n$, let w be n root of 1 in $\bmod q$, it makes w_j into $w^{j-1} \bmod q$, in $1 < j < n$, it shall fill $w_j \neq 1$.

It assigns each decoding person P_j a value w_j , let the decoding person's P_j secret key $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ be the secret value corresponding to a value w_j acquired by dispersing (x_1, x_2, y_1, y_2, z) with the secret dispersion method of threshold-value t which satisfies $3 \leq t < n$,

Let $X_j = g_1^{x_{1j}} g_2^{x_{2j}} \bmod p$, $Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p$, and $Z_j = g_1^{z_j} \bmod p$ be the decoding person's P_j public key (X_j, Y_j, Z_j) , a safe communication channel shall be between each decoding person apparatus.

Moreover, that each decoding person apparatus receives the content with all the members' same

各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路を利用できるものとし、

乱数 $r \in Z_q$ をしきい値 t の秘密分散法により分散して得られる、値 w_j に対応する秘密値 r_j を復号者 P_j は保持するものとし、

各復号者 P_j の装置は、 $r \cdot x_1$, $r \cdot x_2$, $r \cdot y_1$, $r \cdot y_2$ をそれぞれしきい値 t の秘密分散法により分散して得られる、値 w_j に対応する秘密値 $x_{1j'}$, $x_{2j'}$, $y_{1j'}$, $y_{2j'}$ を分散乗算法によって計算して保持し、

暗号文を受信した各復号者 P_j の装置は、 $c = H(u_1, u_2)$ を計算し、 $V_j = u_1^{x_{1j'} + cy_{1j'}} u_2^{x_{2j'} + cy_{2j'}} v^{-r_j} \bmod p$ を計算し、放送型通信路により、 V_j を他の全ての復号者装置へ送信し、 (V_1, \dots, V_n) の指数部が BCH 符号のコードワードであることを確認し、

指数部に対する秘密復元手順により復元した値 V が 1 に等しいことを確認することによって暗号文の正当性を検証することを特徴とする暗号文検証方法。

【請求項 10】

請求項 9 の暗号文検証方法において、

other decoding person apparatus shall utilize the broadcast type communication channel guaranteed.

The decoding person P_j shall maintain the secret value r_j corresponding to a value w_j acquired by dispersing random-number r (element of Z_q) with the secret dispersion method of threshold-value t .

Each decoding person's P_j apparatus calculates and maintains secret value $x_{1j'}$ corresponding to a value w_j obtained by each dispersing $r \cdot x_1$, $r \cdot x_2$, $r \cdot y_1$, and $r \cdot y_2$ with the secret dispersion method of threshold-value t , $x_{2j'}$, $y_{1j'}$, and $y_{2j'}$ by the distributed multiplying method,

The apparatus of each decoding person P_j who received the cryptogram calculates $c = H(u_1, u_2)$, it calculates $V_j = u_1^{x_{1j'} + cy_{1j'}} u_2^{x_{2j'} + cy_{2j'}} v^{-r_j} \bmod p$, according to a broadcast type communication channel, it transmits V_j to all other decoding person apparatus, it checks that the index part of (V_1, \dots, V_n) is the coding word of a BCH code, it verifies the correctness of a cryptogram by checking that the value V decompressed with the secret decompression procedure with respect to an index part is equal to 1.

[CLAIM 10]

A cryptogram verification method, in which in the cryptogram verification method of Claim 9, it

しきい値 t を $2 \leq t \leq n$ を満たすものとし、 (V_1, \dots, V_n) の指数部が BCH 符号のコードワードであることを確認する代わりに、各復号者 P_j の装置が、 V_j が $u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-rj} \bmod p$ の正しい計算結果であることを $x1j'$, $x2j'$, $y1j'$, $y2j'$, rj に関する情報を漏らすことなく、零知識証明によって他の復号者装置に証明し、零知識証明が失敗した復号者 P_j を逸脱者として特定し、逸脱者の秘密値 $x1j'$, $x2j'$, $y1j'$, $y2j'$, rj を他の復号者装置が秘密値回復手順を用いて復元することを特徴とする暗号文検証方法。

【請求項 11】

請求項 9 の暗号文検証方法において、

(V_1, \dots, V_n) が BCH 符号のコードワードでない場合に、各復号者 P_j の装置は、 V_j が $u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-rj} \bmod p$ の計算結果であることを $x1j'$, $x2j'$, $y1j'$, $y2j'$, rj に関する情報を漏らすことなく、零知識証明によって他の復号者装置に証明し、証明に失敗した復号者 P_j の装置を逸脱者の装置と特定し、逸脱者の装置の秘密値 $x1j'$, $x2j'$, $y1j'$, $y2j'$, rj を他の復号者装置が秘密値回復手順を用いて復元することを特徴とする暗号文検証方法。

shall fill $2 \leq t \leq n$ for threshold-value t .

Instead of checking that the index part of (V_1, \dots, V_n) is the coding word of a BCH code, each decoding person's P_j apparatus

Without V_j leaks the information concerning that it is the correct calculation result of $u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-rj} \bmod p$, and $[x1j', x2j', y1j', y2j', rj]$, it proves to another decoding person apparatus by zero knowledge proof, it specifies the decoding person P_j in whom zero knowledge proof failed as a deviation person, another decoding person apparatus decompresses a deviation person's secret value $x1j'$, $x2j'$, $y1j'$, $y2j'$, and rj using a secret value recovery procedure.

[CLAIM 11]

In the cryptogram verification method of Claim 9, when (V_1, \dots, V_n) are not the coding words of a BCH code, it proves each decoding person's P_j apparatus to another decoding person apparatus by zero knowledge proof, without leaking the information concerning [that V_j is the calculation result of $u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-rj} \bmod p$, and $[x1j', x2j', y1j', y2j', rj]$, it specifies the apparatus of the decoding person P_j who failed in proof with a deviation person's apparatus, another decoding person apparatus decompresses secret value $x1j'$ of a deviation person's apparatus, $x2j'$, $y1j'$, $y2j'$, and rj using a secret value recovery procedure.

The cryptogram verification method

$y_{2j'}$, r_j を、他の復号者装置が秘密値回復手順を用いて復元することを特徴とする暗号文検証方法。

characterized by the above-mentioned.

【請求項 12】

請求項 9 の暗号文検証方法において、
上記復元した値 V が 1 に等しい場合に、各復号者 P_j の装置は $D_j = u_1^{z_j} \bmod p$ を計算し、放送型通信路により他の全ての復号者装置へ送信し、
受信した (D_1, \dots, D_n) の u_1 を底とする離散対数が BCH 符号のコードワードであることを確認することを特徴とする暗号文検証方法。

[CLAIM 12]

A cryptogram verification method, in which in the cryptogram verification method of Claim 9, when the above-mentioned value V which decompressed is equal to 1, each decoding person's P_j apparatus calculates $D_j = u_1^{z_j} \bmod p$, it transmits to all other decoding person apparatus according to a broadcast type communication channel, it checks that the discrete logarithm which uses as a bottom u_1 which received (D_1, \dots, D_n) is the coding word of a BCH code.

【請求項 13】

請求項 10 の暗号文検証方法において、
復元した値 V が 1 に等しい場合に、各復号者 P_j の装置は $D_j = u_1^{z_j} \bmod p$ を計算し、 D_j が正しい計算結果であることを z_j に関する情報を漏らすことなく、零知識証明によって他の復号者に証明し、
零知識証明に失敗した復号者 P_j を逸脱者として特定し、逸脱者の秘密値 z_j を他の復号者装置が秘密値回復手順を用いて復元することを特徴とする暗号文検証方法。

[CLAIM 13]

A cryptogram verification method, in which in the cryptogram verification method of Claim 10, in each decoding person's P_j apparatus, the decompressed value V calculates $D_j = u_1^{z_j} \bmod p$, when equal to 1, d_j is the correct calculation result.

Without it leaks the information about z_j , it proves to another decoding person by zero knowledge proof, it specifies the decoding person P_j who failed in zero knowledge proof as a deviation person, another decoding person apparatus decompresses a deviation person's secret value z_j using a secret value recovery procedure.

【請求項 14】

請求項 12 又は 13 の暗号文
検証方法において、
各復号者装置は正しい (D_1 ,
..., D_n) から、
 u_1 を底とする指数部に対する
秘密復元手順により $D = u_1^z \bmod p$
を復元し、
 $m = e / D \bmod p$ を計算して
平文 m を復号することを特徴と
する暗号文検証方法。

【請求項 15】

p を大きな素数、 q を $p-1$
を割り切る大きな素数とし、 G
 q は乗法群 Z_p の位数 p の部分
群を表すものとし、 g_1 , g_2
を G_p の元とし、 H を汎用ハッ
シュ関数とし、 $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $Z = g_1^z \bmod p$ を暗号化
手順に用いる公開鍵とし、 $(x_1, x_2, y_1, y_2, z) \in Z_q^5$ とし、平文 m に対する暗
号文 E は c を $H(u_1, u_2)$
 $\bmod p$ として $u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $v = X^r Y^{cr} \bmod p$ なる三つ組み(u_1, u_2, v) を含み、
乱数 r を生成する処理と、
暗号文 E を受信する処理と、
 $c = H(u_1, u_2) \bmod q$ を
計算する処理と、

$V = (u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$ を計算する処理と、

[CLAIM 14]

A cryptogram verification method, in which in
the cryptogram verification method of Claim 12
or 13, from it being correct (D_1 ..., D_n), each
decoding person apparatus decompresses
 $D = u_1^z \bmod p$ with the secret decompression
procedure with respect to the index part which
uses u_1 as a bottom, calculates $m = e / D \bmod p$,
and decodes Plaintext m .

[CLAIM 15]

It considers it as the big prime number which
gives a clear-cut solution for p to a big prime
number, and gives a clear-cut solution for q to
 $p-1$, g_1, g_2 shall express the partial group of the
digit p of multiplicative group Z_p .

It carries out g_1 and g_2 the origin of G_p , let H be
a general purpose hash function, let
 $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, and $Z = g_1^z \bmod p$ be the public key which it uses for an
encryption procedure, (x_1, x_2, y_1, y_2, z) It
considers it as (element of) Z_q^5 , the cryptogram
 E with respect to Plaintext m

It is considering c as $H(u_1, u_2) \bmod p$.

The 3 sets (u_1, u_2, v) used as $u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $v = X^r Y^{cr} \bmod p$ are included,
processing which forms a random number r ,
processing which receives Cryptogram E ,
processing which calculates $c = H(u_1, u_2) \bmod q$,

$V =$ (processing which calculates
 $u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$)

V = 1であることを確認して暗号文の正当性を検証する処理とを復号者装置のコンピュータに実行させるプログラムを記録した記録媒体。

【請求項 16】

V ≠ 1 ならば、ビットコミットメント関数 (BC) を用いて BC (r) を公開する処理と、BC (r) を構成する r と、公開鍵 X, Y を構成する x₁, x₂, y₁, y₂ を用いて、 $(u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$ なる計算を行った結果が V であることを、r, x₁, x₂, y₁, y₂ に関する秘密を漏らさずに零知識証明で第三者へ証明する処理とを実行させるプログラムを含むことを特徴とする記録媒体。

【請求項 17】

p を大きな素数、q を p - 1 を割り切る大きな素数とし、G_q は乗法群 Z_p の位数 q の部分群を表すものとし、g₁, g₂ を G_q の元とし、H を汎用ハッシュ関数とし、n 人の復号者を P₁ ~ P_n とし、各復号者 P_j は固有の公開値 w_j を持ち、 $(x_1, x_2, y_1, y_2, z) \in Z_q^5$ を、 $3 \leq t \leq n$ を満たすしきい値 t の秘密分散法により分散して得られる、値 w_j に対応する秘密値 (x_{1j}, x_{2j},

The recording medium on which was recorded the program which lets the computer of a decoding person apparatus perform processing which checks that it is V = 1 and verifies the correctness of a cryptogram.

[CLAIM 16]

Processing which will exhibit BC (r) using bit commitment function (BC) if it becomes V ≠ 1, r which comprises BC(r), it uses x₁, x₂, y₁, and y₂ which comprise public key X and Y, the result of having performed calculation used as $(u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$ is V, the recording medium characterized by including the program which performs processing which it proves to a third person by zero knowledge proof without leaking the secret about r, x₁, x₂, y₁, y₂.

[CLAIM 17]

It considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to p-1, g_q shall express the partial group of the digit q of multiplicative group Z_p.

It carries out g₁ and g₂ the origin of G_q, let H be a general purpose hash function, it sets n persons' decoding person to P₁-P_n, let the secret value (x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j) corresponding to a value w_j which each decoding person P_j has the inherent open value w_j, and is acquired by dispersing (element of) $(x_1, x_2, y_1, y_2, z) \in Z_q^5$ with the secret

y_{1j}, y_{2j}, z_j) を復号者 P_j の秘密鍵とし、 $X_j = g^{x_{1j}} g^{x_{2j}} \bmod p$, $Y_j = g^{y_{1j}} g^{y_{2j}} \bmod p$, $Z_j = g^{z_j} \bmod p$ を復号者 P_j の公開鍵とし、

乱数 $r \in \mathbb{Z}_q$ をしきい値 t の秘密分散法により分散して得られる値 w_j に対応する秘密値 r_j を生成する処理と、

$X = g^{x_1} g^{x_2} \bmod p$, $Y = g^{y_1} g^{y_2} \bmod p$, $Z = g^{z_j} \bmod p$ を公開鍵とし、平文 m の暗号文とし、正しい暗号文は $u_1 = g^{r_1} \bmod p$, $u_2 = g^{r_2} \bmod p$, $c = H(u_1, u_2)$, $v = X^r Y^{cr} \bmod p$, $e = m Z^r \bmod p$ を満たして暗号文 $E = (u_1, u_2, v, e)$ を受信する処理と、

$c = H(u_1, u_2)$ を計算する処理と、

$V_j = (u_1^{x_{1j}+cy_{1j}} u_2^{x_{2j}+cy_{2j}} v^{-1})^{r_j} \bmod p$ を計算する処理と、

V_j をしきい値 t 以上 $2t$ 以下の検証可能秘密分散法により分散して得られる、値 w_k に対応する秘密値 V_{jk} を各復号者 P_k の装置に送信する処理と、他の全ての復号者装置 P_k から V_{kj} を受信する処理と、 V_j を他の全ての復号者装置へ送信する処理と、

他の全ての復号者装置から V_k

dispersion method of threshold-value t which fills $3t < n$ be the decoding person's P_j secret key, let $X_j = g^{x_{1j}} g^{x_{2j}} \bmod p$, $Y_j = g^{y_{1j}} g^{y_{2j}} \bmod p$, and $Z_j = g^{z_j} \bmod p$ be the decoding person's P_j public key, processing which forms the secret value r_j corresponding to the value w_j obtained by dispersing random-number r (element of) \mathbb{Z}_q with the secret dispersion method of threshold-value t , let $X = g^{x_1} g^{x_2} \bmod p$, $Y = g^{y_1} g^{y_2} \bmod p$, and $Z = g^{z_j} \bmod p$ be public key, it considers it as the cryptogram of Plaintext m , the correct cryptogram is processing which fills $u_1 = g^{r_1} \bmod p$, $u_2 = g^{r_2} \bmod p$, $c = H(u_1, u_2)$, $v = X^r Y^{cr} \bmod p$, and $e = m Z^r \bmod p$, and receives cryptogram $E = (u_1, u_2, v, e)$, processing which calculates $c = H(u_1, u_2)$,

$V_j =$ (processing which calculates $u_1^{x_{1j}+cy_{1j}} u_2^{x_{2j}+cy_{2j}} v^{-1})^{r_j} \bmod p$)

Processing which transmits the secret value V_{jk} corresponding to a value w_k acquired by dispersing V_j with t or more threshold values and a verifiable secret dispersion method $2t$ or less to each decoding person's P_k apparatus, processing which receives V_{kj} from all other decoding person apparatus P_k , processing which transmits V_j to all other decoding person apparatus,

Processing which receives V_k from all other

を受信する処理と、
 V_{kj} を他の全ての復号者装置へ送信する処理と、
 各 V_k が正しい値であることを他の全ての復号者装置からの V_{kj} を用いて検証する処理と、
 正しいと確認された V_k のうち $2t+1$ 個を選択し、指数部に対する秘密復元手順により復元した値 V が 1 に等しいか否かを調べ、等しくないならば他の $2t+1$ 個の組み合わせで同様に秘密復元手順を繰り返し、全ての組み合わせについていずれも復元値が 1 に等しくないなら、その暗号文を不正と判定し、一つでも 1 になる組み合わせがあったならば、その暗号文を正しいと判定する処理と、を復号者装置のコンピュータに実行させるプログラムを記録した記録媒体。

【請求項 18】

p を大きな素数、 q を $p-1$ を割り切る大きな素数とし、 G_q は乗法群 Z_p の位数 q の部分群を表すものとし、 g_1, g_2 を G_q の元とし、 H を汎用ハッシュ関数とし、
 $(x_1, x_2, y_1, y_2, z) \in Z_{q^5}$ を秘密鍵、 $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $Z = g_1^z \bmod p$ なる (X, Y, Z) を公開鍵とし、平文 m に対する暗号文 E は c を

decoding person apparatus, processing which transmits V_{kj} to all other decoding person apparatus, processing which verifies that each V_k is the correct value using V_{kj} from all other decoding person apparatus, if correct, it will choose $2t+1$ piece among checked $V_k(s)$, it examines whether the value V decompressed with the secret decompression procedure with respect to an index part is equal to 1, if not equal

It repeats a secret decompression procedure similarly in other $2t+1$ piece combination, about all combination, if the decompression value is not all equal to 1, it will judge that the cryptogram is irregular, the recording medium on which was recorded the program which will let the computer of a decoding person apparatus perform processing which judges that the cryptogram is correct if there is combination set to 1 at least one.

[CLAIM 18]

It considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to $p-1$, G_q shall express the partial group of the digit q of multiplicative group Z_p .

It carries out g_1 and g_2 the origin of G_q , let H be a general purpose hash function, (x_1, x_2, y_1, y_2, z)

Let a secret key, $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, and $Z = g_1^z \bmod p$ be public key for (element of) Z_{q^5} (X, Y, Z) , the 3 sets (u_1, u_2, v) which the cryptogram E with respect

$H(u_1, u_2) \bmod q$ として to Plaintext m makes $c = H(u_1, u_2) \bmod q$, and
 $u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $v = X^r Y^{cr} \bmod p$ constitute $u_1 = g_1^r \bmod p, u_2 = g_2^r \bmod p, v = X^r Y^{cr} \bmod p$ are included, processing which forms
 なる三つ組み (u_1, u_2, v) a random number r ,
 を含み、
 乱数 r を生成する処理と、

上記 r を用いて $x_1' = x_1 \cdot r \bmod q$, $x_2' = x_2 \cdot r \bmod q$, $y_1' = y_1 \cdot r \bmod q$, $y_2' = y_2 \cdot r \bmod q$ を
 計算する処理と、
 暗号文 E を受信する処理と、
 受信した暗号文から、 $c = H(u_1, u_2) \bmod q$ を計算し、 $V = u_1^{x_1' + cy_1'} u_2^{x_2' + cy_2'} v^{-r} \bmod p$ を計算する処理と、
 上記 V が 1 に等しいことを確認
 することによって暗号文の正当
 性を検証する処理とを復号者装
 置のコンピュータに実行させる
 プログラムを記録した記録媒
 体。

【請求項 19】

請求項 18 の記録媒体におい
 て、
 V が 1 に等しくない場合に、
 (X, Y, V) が、ある (x_1, x_2, y_1, y_2, r) に対し
 て $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $V = u_1^{x_1 + cy_1} u_2^{x_2 + cy_2} v^{-r} \bmod p$
 を満足することを零知識証明を
 用いて (x_1, x_2, y_1, y_2, r) を秘密としたまま検証

Processing which calculates $x_1' = x_1$ and $r \bmod q$,
 $x_2' = x_2$ and $r \bmod q$, $y_1' = y_1$ and $r \bmod q$, and
 $y_2' = y_2$ and $r \bmod q$ using the above-mentioned r ,
 processing which receives Cryptogram E , from
 the cryptogram which received, it calculates
 $c = H(u_1, u_2) \bmod q$, processing which calculates
 $V = u_1^{x_1' + cy_1'} u_2^{x_2' + cy_2'} v^{-r} \bmod p$, the recording
 medium on which was recorded the program
 which lets the computer of a decoding person
 apparatus perform processing which verifies the
 correctness of a cryptogram when the
 above-mentioned V checks that it is equal to 1.

[CLAIM 19]

In the recording medium of Claim 18, in V , to the
 case of not being equal to 1, (X, Y, V) are
 $X = g_1^{x_1} g_2^{x_2} \bmod p$ for it being (x_1, x_2, y_1, y_2, r) ,
 $y = g_1^{y_1} g_2^{y_2} \bmod p$, use zero knowledge proof for
 satisfying $V = u_1^{x_1 + cy_1} u_2^{x_2 + cy_2} v^{-r} \bmod p$.
 Have made secret (x_1, x_2, y_1, y_2, r) .
 The recording medium characterized by the
 above-mentioned program including the
 program which lets the above-mentioned
 computer perform processing which it proves to
 a verification person.

者に証明する処理を上記コンピュータに実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

【請求項 20】

請求項 19 の記録媒体において、

g, h は g を底とする h の離散対数が未知であるような G_q の元であって、

乱数 r, a_1, a_2, b_1, b_2 を生成する処理と、

$R = g^r h^a \bmod p, RX1 = R^{x1} h^{a1} \bmod p, RX2 = R^{x2} h^{a2} \bmod p, RY1 = R^{y1} h^{b1} \bmod p, RY2 = R^{y2} h^{b2} \bmod p$ なる $R, RX1, RX2, RY1, RY2$ を公開する処理と、

$(X, Y, V, R, RX1, RX2, RY1, RY2)$ がある $(x1, x2, y1, y2, r, a, a1, a2, b1, b2)$ に対して、

$X = g^{x1} g^{x2} \bmod p, Y = g^{y1} g^{y2} \bmod p, V = u^{x1r+cy1r} u^{x2r+cy2r} v^{-r} \bmod p, R = g^r h^a \bmod p, RX1 = R^{x1} h^{a1} \bmod p, RX2 = R^{x2} h^{a2} \bmod p, RY1 = R^{y1} h^{b1} \bmod p, RY2 = R^{y2} h^{b2} \bmod p$ なる関係式を満たすことを零知識証明によって証明する処理とを上記コンピュータ

[CLAIM 20]

In the recording medium of Claim 19, g and h are under G_q whose discrete logarithm of h which uses g as a bottom is unknown, comprised such that processing which forms random numbers r, a_1, a_2, b_1 , and b_2 , processing which exhibits $R, RX1, RX2, RY1$, and $RY2$ used as $R = g^r h^a \bmod p, RX1 = R^{x1} h^{a1} \bmod p, RX2 = R^{x2} h^{a2} \bmod p, RY1 = R^{y1} h^{b1} \bmod p, RY2 = R^{y2} h^{b2} \bmod p$,

To $(x1, x2, y1, y2, r, a, a1, a2, b1, b2)$ with $(X, Y, V, R, RX1, RX2, RY1, RY2), x = g^{x1} g^{x2} \bmod p, y = g^{y1} g^{y2} \bmod p, v = u^{x1r+cy1r} u^{x2r+cy2r} v^{-r} \bmod p, r = g^r h^a \bmod p, RX1 = R^{x1} h^{a1} \bmod p, RX2 = R^{x2} h^{a2} \bmod p, RY1 = R^{y1} h^{b1} \bmod p$, the recording medium characterized by the above-mentioned program including the program which lets the above-mentioned computer perform processing which proves filling the relation used as $RY2 = R^{y2} h^{b2} \bmod p$ by zero knowledge proof.

に実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

【請求項 21】

請求項 18 の記録媒体において、

n 人の復号者を $P_1 \sim P_n$ とし、 w を $\text{mod } q$ での 1 の n 乗根とし、 w_j を $w^{j-1} \text{ mod } q$ とし、 $1 < j < n$ において $w_j \neq 1$ を満たすものとし、各復号者 P_j に値 w_j を割り当て、復号者 P_j の秘密鍵 $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ は、 $3 \leq t < n$ を満たすしきい値 t の秘密分散法により (x_1, x_2, y_1, y_2, z) を分散して得られる、値 w_j に対応する秘密値とし、

$X_j = g^{x_{1j}} g^{x_{2j}} \text{ mod } p$,
 $Y_j = g^{y_{1j}} g^{y_{2j}} \text{ mod } p$,
 $Z_j = g^{z_j} \text{ mod } p$ なる (X_j, Y_j, Z_j) を復号者 P_j の公開鍵とし、

乱数 $r \in \mathbb{Z}_q$ をしきい値 t の秘密分散法により分散して得られる、値 w_j に対応する秘密値 r_j を保持する処理と、

rx_1, rx_2, ry_1, ry_2 をそれぞれしきい値 t の秘密分散法により分散して得られる、値 w_j に対応する秘密値 $x_{1j}', x_{2j}', y_{1j}', y_{2j}'$ を分散乗算法によって

[CLAIM 21]

In the recording medium of Claim 18, it sets n persons' decoding person to $P_1 \sim P_n$, let w be n root of 1 in $\text{mod } q$, it makes w_j into $w^{j-1} \text{ mod } q$, in $1 < j < n$, it shall fill $w_j \neq 1$.

It assigns each decoding person P_j a value w_j , let the decoding person's P_j secret key $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ be the secret value corresponding to a value w_j acquired by dispersing (x_1, x_2, y_1, y_2, z) with the secret dispersion method of threshold-value t which fills $3 \leq t < n$, let $X_j = g^{x_{1j}} g^{x_{2j}} \text{ mod } p$, $Y_j = g^{y_{1j}} g^{y_{2j}} \text{ mod } p$, and $Z_j = g^{z_j} \text{ mod } p$ be the decoding person's P_j public key (X_j, Y_j, Z_j) ,

Processing holding the secret value r_j corresponding to a value w_j acquired by dispersing random-number r (element of \mathbb{Z}_q) with the secret dispersion method of threshold-value t , processing which calculates and maintains secret value $x_{1j}', x_{2j}', y_{1j}', y_{2j}'$ corresponding to a value w_j obtained by each dispersing rx_1, rx_2, ry_1, ry_2 with the secret dispersion method of threshold-value t by the distributed multiplying method, reception of a cryptogram

計算して保持する処理と、
暗号文を受信すると、 $c = H(u_1, u_2)$ を計算し、 $V_j = u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-rj} \bmod p$ を計算し、放送型通信路により、 V_j を他の全ての復号者装置へ送信する処理と、

(V_1, \dots, V_n) の指数部が BCH 符号のコードワードであることを確認する処理と、

上記指数部に対する秘密復元手順により復元した値 V が 1 に等しいことを確認することによって暗号文の正当性を検証する処理とを上記コンピュータにより実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

【請求項 22】

請求項 21 の記録媒体において、

しきい値 t を $2 \leq t < n$ を満たすものとし、

(V_1, \dots, V_n) の指数部が BCH 符号のコードワードであることを確認する処理の代わりに、 V_j が $u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-rj} \bmod p$ の正しい計算結果であることを $x1j', x2j', y1j', y2j', rj$ に関する情報を漏らすことなく、零知識証明によって他の復号者に証明する処理と、
零知識証明が失敗した復号者 P

will calculate $c = H(u_1, u_2)$, it calculates $V_j = u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-rj} \bmod p$, processing which transmits V_j to all other decoding person apparatus according to a broadcast type communication channel, processing which checks that the index part of (V_1, \dots, V_n) is the coding word of a BCH code,

The recording medium characterized by the above-mentioned program including the program which performs processing which verifies the correctness of a cryptogram by checking that the value V decompressed with the secret decompression procedure with respect to the above-mentioned index part is equal to 1 by above-mentioned computer.

[CLAIM 22]

In the recording medium of Claim 21, it shall fill $2 \leq t < n$ for threshold-value t .

Instead of the processing which checks that the index part of (V_1, \dots, V_n) is the coding word of a BCH code], without V_j leaks the information concerning that it is the correct calculation result of $u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-rj} \bmod p$, and $] x1j', x2j', y1j', y2j', rj$, processing which it proves to another decoding person by zero knowledge proof, it specifies the decoding person P_j in whom zero knowledge proof failed as a deviation person, the recording medium characterized by including the program which lets the above-mentioned computer perform a deviation person's secret value $x1j', x2j', y1j'$,

j を逸脱者として特定し、逸脱者の秘密値 $x_{1j'}$, $x_{2j'}$, $y_{1j'}$, $y_{2j'}$, r_j を秘密値回復手順を用いて復元する処理とを上記コンピュータに実行させるプログラムを上記プログラムに含むことを特徴とする記録媒体。

【請求項 23】

請求項 21 の記録媒体において、

(V_1, \dots, V_n) が BCH 符号のコードワードでない場合に、 V_j が $u_1^{x_{1j'}+cy_{1j'}} u_2^{x_{2j'}+cy_{2j'}} v^{-r_j} \bmod p$ の計算結果であることを $x_{1j'}$, $x_{2j'}$, $y_{1j'}$, $y_{2j'}$, r_j に関する情報を漏らすことなく、零知識証明によって他の復号者に証明する処理と、上記証明に失敗した復号者 P_j を逸脱者と特定し、逸脱者の秘密値 $x_{1j'}$, $x_{2j'}$, $y_{1j'}$, $y_{2j'}$, r_j を、秘密値回復手順を用いて復元する処理とを上記コンピュータに実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

【請求項 24】

p を大きな素数、 q を $p-1$ を割り切る大きな素数とし、 G_q は乗法群 Z_p の位数 q の部分群を表すものとし、 g_1 , g_2 を G_q の元とし、 H を汎用ハッシュ関数とし、

$y_{2j'}$, and processing that decompresses r_j using a secret value recovery procedure in the above-mentioned program.

[CLAIM 23]

In the recording medium of Claim 21, when (V_1, \dots, V_n) are not the coding words of a BCH code, without it leaks the information concerning that V_j is the calculation result of $u_1^{x_{1j'}+cy_{1j'}} u_2^{x_{2j'}+cy_{2j'}} v^{-r_j} \bmod p$, and $x_{1j'}, x_{2j'}, y_{1j'}, y_{2j'}, r_j$, it specifies the processing which it proves to another decoding person by zero knowledge proof, and the decoding person P_j who failed in the above-mentioned proof with a deviation person, the recording medium characterized by the above-mentioned program including the program which lets the above-mentioned computer perform processing which decompresses a deviation person's secret value $x_{1j'}, x_{2j'}, y_{1j'}, y_{2j'}$, and r_j using a secret value recovery procedure.

[CLAIM 24]

A cryptogram verification apparatus, which considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to $p-1$, g_q shall express the partial group of the

シユ関数とし、

$(x_1, x_2, y_1, y_2, z) \in Z_q^5$ を秘密鍵、 $X = g^{x_1} g^{x_2} \bmod p$, $Y = g^{y_1} g^{y_2} \bmod p$, $Z = g^{z_1} \bmod p$ なる (X, Y, Z) を公開鍵とし、平文 m に対する暗号文 E は c を $H(u_1, u_2) \bmod q$ として $u_1 = g^{r_1} \bmod p$, $u_2 = g^{r_2} \bmod p$, $v = X^{r_1} Y^{r_2} \bmod p$ なる三つ組み (u_1, u_2, v) を含む暗号文の検証装置であつて、

乱数 r を生成する手段と、

$c = H(u_1, u_2) \bmod q$ を計算する手段と、

$V = (u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$ を計算する手段と、

V が 1 に等しいことを確認することによって暗号文の正当性を検証する手段とを備えることを特徴とする暗号文検証装置。

【請求項 25】

請求項 24 の暗号文検証装置において、

V が 1 に等しくない場合に、零知識証明を用いて第三者に V が乱数 r に対して $(u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$ のように計算した結果であることを証明する手段を備えることを特徴とする暗号文検証装置。

【請求項 26】

digit q of multiplicative group Z_p .

It carries out g_1 and g_2 the origin of G_q , let H be a general purpose hash function, (x_1, x_2, y_1, y_2, z)

Let a secret key, $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, and $Z = g_1^{z_1} \bmod p$ be public key for (element of) Z_q^5 (X, Y, Z) , the cryptogram E with respect to Plaintext m is considering c as $H(u_1, u_2) \bmod q$.

It is the verification apparatus of the cryptogram containing the 3 sets (u_1, u_2, v) used as $u_1 = g_1^{r_1} \bmod p$, $u_2 = g_2^{r_2} \bmod p$, $v = X^{r_1} Y^{r_2} \bmod p$, comprised such that means to form a random number r ,

Means to calculate $c = H(u_1, u_2) \bmod q$, means to calculate $V = (u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$,

means to verify the correctness of a cryptogram when V checks that it is equal to 1

Are provided.

[CLAIM 25]

A cryptogram verification apparatus, in which in the cryptogram verification apparatus of Claim 24, when V is not equal to 1, v receives a third person at a random number r using zero knowledge proof (it has means to prove that it is the result of calculating like $u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$).

[CLAIM 26]

p を大きな素数、 q を $p-1$ を割り切る大きな素数とし、 G_q は乗法群 Z_p の位数 q の部分群を表すものとし、 g_1, g_2 を G_q の元とし、 H を汎用ハッシュ関数とし、

n 人の復号者を $P_1 \sim P_n$ とし、各復号者 P_j は固有の公開値 w_j を持ち、

$(x_1, x_2, y_1, y_2, z) \in Z_q^5$ を、 $3 \leq t \leq n$ を満たすしきい値 t の秘密分散法により分散して得られる、値 w_j に対応する秘密値 $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ を復号者 P_j の秘密鍵とし、

$X_j = g_1^{x_{1j}} g_2^{x_{2j}} \bmod p$,
 $Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p$,
 $Z_j = g_1^{z_j} \bmod p$ なる (X_j, Y_j, Z_j) を復号者 P_j の公開鍵とし、

各々の復号者装置間には、安全な通信路があるものとし、また、各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路を利用できるものとし、乱数 $r \in Z_q$ をしきい値 t の秘密分散法により分散して得られる、値 w_j に対応する秘密値 r_j を復号者 P_j は保持するものとし、

$E = (u_1, u_2, v, e)$ を、
 $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $Z = g_1^z$

A cryptogram verification apparatus, which considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to $p-1$, g_1, g_2 shall express the partial group of the digit q of multiplicative group Z_p .

It carries out g_1 and g_2 the origin of G_q , let H be a general purpose hash function, it sets n persons' decoding person to P_1-P_n , each decoding person P_j has the inherent open value w_j , let the secret value $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ corresponding to a value w_j acquired by dispersing (x_1, x_2, y_1, y_2, z) (element of) Z_q^5 with the secret dispersion method of threshold-value t which fills $3 \leq t \leq n$ be the decoding person's P_j secret key, let $X_j = g_1^{x_{1j}} g_2^{x_{2j}} \bmod p$, $Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p$, and $Z_j = g_1^{z_j} \bmod p$ be the decoding person's P_j public key (X_j, Y_j, Z_j) ,

A safe communication channel shall be between each decoding person apparatus.

Moreover, that each decoding person apparatus receives the content with all the members' same other decoding person apparatus shall utilize the broadcast type communication channel guaranteed.

The decoding person P_j shall maintain the secret value r_j corresponding to a value w_j acquired by dispersing random-number r (element of) Z_q with the secret dispersion method of threshold-value t .

Let $E = (u_1, u_2, v, e)$ be a cryptogram with respect to plaintext m which used

mod p を公開鍵とした平文 m に対する暗号文とし、正しい暗号文は $u_1 = g_1^r \text{ mod } p$, $u_2 = g_2^r \text{ mod } p$, $c = H(u_1, u_2)$, $v = X^r Y^{cr} \text{ mod } p$, $e = m Z^r \text{ mod } p$ を満足する暗号文の検証装置であって、 E を受信して $c = H(u_1, u_2)$ を計算する手段と、

$V_j = (u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-1})^{rj} \text{ mod } p$ を計算する手段と、 V_j をしきい値 t 以上 $2t$ 以下の検証可能秘密分散法により分散して、値 w_k に対応する秘密値 V_{jk} を得る手段と、 V_{jk} を各復号者 P_k の装置に安全な通信路を介して送信する手段と、他の全ての復号者装置 P_k から V_{kj} を受信すると、放送型通信路により、 V_j を他の全ての復号者装置へ送信する手段と、

V_k を受信すると、対応する V_{kj} を放送型通信路により他の全ての復号者装置へ送信する手段と、各 V_k が正しい値であることを V_{kj} を用いて検証する手段と、正しいと確認された V_k のうち $2t+1$ 個を選択し、指数部に対する秘密復元手順により V を復元する手段と、復元した値 V が 1 に等しいか否

$X = g_1^{x1} g_2^{x2} \text{ mod } p$, $Y = g_1^{y1} g_2^{y2} \text{ mod } p$, and $Z = g_1^z \text{ mod } p$ as public key, the correct cryptogram is the verification apparatus of the cryptogram which satisfies $u_1 = g_1^r \text{ mod } p$, $u_2 = g_2^r \text{ mod } p$, $c = H(u_1, u_2)$, $v = X^r Y^{cr} \text{ mod } p$, and $e = m Z^r \text{ mod } p$, comprised such that means to calculate $c = H(u_1, u_2)$ by receiving E ,

$V_j = (u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-1})^{rj} \text{ mod } p$ (means to calculate $u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-1})^{rj} \text{ mod } p$)

It disperses V_j with t or more threshold values and a verifiable secret dispersion method $2t$ or less, means to acquire the secret value V_{jk} corresponding to a value w_k , means to transmit V_{jk} through a communication channel safe for each decoding person's P_k apparatus, means to transmit V_j to all other decoding person apparatus according to a broadcast type communication channel if V_{kj} is received from all other decoding person apparatus P_k ,

Means to transmit corresponding V_{kj} to all other decoding person apparatus according to a broadcast type communication channel if V_k is received, means by which each V_k verifies using V_{kj} that it is the correct value, if correct, it will choose $2t+1$ piece among checked $V_k(s)$, means to decompress V with the secret decompression procedure with respect to an index part, means to examine whether the decompressed value V is equal to 1,

かを調べる手段と、

Vが1に等しくないならば他の
 $2t+1$ 個の組み合わせで同様に
 秘密復元手順を繰り返し、V
 が1に等しいか否かを調べる手段
 と、
 $2t+1$ 個の全ての組み合わせ
 についていずれも復元値が1に
 等しくないならば、その暗号文
 を不正と判定し、一つでも1に
 なる組み合わせがあったなら
 ば、その暗号文を正しいと判定
 する手段と、を備えることを特
 徴とする暗号文検証装置。

【請求項27】

請求項26の暗号文検証装置
 において、
 w を $\text{mod } q$ での1の n 乗根と
 し、各復号者は、 w^j を $w^{j-1} \text{ mod } q$
 とし、 $1 < j < n$ において w^j
 $\neq 1$ を満たすような w^j を公
 開の固有値とし、
 $D_j = u1^{z_j} \text{ mod } p$ を計算する
 手段と、
 D_j を放送型通信路により他の
 全ての復号者装置へ送信する手
 段と、

受信した (D_1, \dots, D_n) の
 $u1$ を底とする離散対数がBC
 H符号のコードワードであるこ
 とを確認する手段とを備えるこ
 とを特徴とする暗号文検証装
 置。

If V is not equal to 1

It repeats a secret decompression procedure
 similarly in other $2t+1$ piece combination,
 means to examine whether V is equal to 1,
 about all $2t+1$ piece combination, if the
 decompression value is not all equal to 1, it will
 judge that the cryptogram is irregular, means to
 judge that the cryptogram is correct if there is
 combination set to 1 at least one

Are provided.

[CLAIM 27]

A cryptogram verification apparatus, in which in
 the cryptogram verification apparatus of Claim
 26, let w be n root of 1 in $\text{mod } q$, each decoding
 person makes w^j $w^{j-1} \text{ mod } q$, it considers it as
 the eigenvalue of public presentation of w^j
 which fills $w^j \neq 1$ in $1 < j < n$, means to calculate
 $D_j = u1^{z_j} \text{ mod } p$, means to transmit D_j to all other
 decoding person apparatus according to a
 broadcast type communication channel,

Means to check that the discrete logarithm
 which uses as a bottom $u1$ which received
 (D_1, \dots, D_n) is the coding word of a BCH code
 Are provided.

【請求項 28】

p を大きな素数、q を p-1 を割り切る大きな素数とし、G_q は乗法群 Z_p の位数 q の部分群を表すものとし、g₁, g₂ を G_q の元とし、H を汎用ハッシュ関数とし、

(x₁, x₂, y₁, y₂, z) ∈ Z_q⁵ を秘密鍵、X = g₁^{x₁} g₂^{x₂} mod p, Y = g₁^{y₁} g₂^{y₂} mod p, Z = g₁^z mod p なる (X, Y, Z) を公開鍵とし、平文 m に対する暗号文 E は c を H(u₁, u₂) mod q として u₁ = g₁^r mod p, u₂ = g₂^r mod p, v = X^r Y^c mod p なる三つ組み (u₁, u₂, v) を含む暗号文の検証装置であって、乱数 r を生成する手段と、

$x_1' = x_1 \cdot r \bmod q$, $x_2' = x_2 \cdot r \bmod q$, $y_1' = y_1 \cdot r \bmod q$, $y_2' = y_2 \cdot r \bmod q$ を計算する手段と、

受信した暗号文から、c = H(u₁, u₂) mod q を計算する手段と、この計算結果と受信暗号文から、 $V = u_1^{x_1'} u_2^{x_2'} v^{-r} \bmod p$ を計算する手段と、

V が 1 に等しいことを確認することによって暗号文の正当性を検証する手段とを備えることを

[CLAIM 28]

A cryptogram verification apparatus, which considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to p-1, g₁, g₂ shall express the partial group of the digit q of multiplicative group Z_p.

It carries out g₁ and g₂ the origin of G_q, let H be a general purpose hash function, (x₁, x₂, y₁, y₂, z).

It is a secret key about (element of) Z_q⁵, it is set to $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $Z = g_1^z \bmod p$.

Let (X, Y, Z) be public key, the cryptogram E with respect to Plaintext m is the verification apparatus of the cryptogram containing the 3 sets (u₁, u₂, v) which constitute u₁ = g₁^r mod p, u₂ = g₂^r mod p, v = X^r Y^c mod p by making c into H(u₁, u₂) mod q, comprised such that means to form a random number r,

Means to calculate $x_1' = x_1$ and r mod q, $x_2' = x_2$ and r mod q, $y_1' = y_1$ and r mod q, and $y_2' = y_2$ and r mod q, means to calculate $c = H(u_1, u_2) \bmod q$ from the cryptogram which received, this calculation result and means to calculate $V = u_1^{x_1'} u_2^{x_2'} v^{-r} \bmod p$ from a receiving cryptogram, means to verify the correctness of a cryptogram when V checks that it is equal to 1 Are provided.

特徴とする暗号文検証装置。

【請求項 29】

請求項 28 の暗号文検証装置において、

V が 1 に等しくない場合に、 (X, Y, V) が、ある (x_1, x_2, y_1, y_2, r) に対して $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $V = u_1^{x_1 r + c y_1 r} u_2^{x_2 r + c y_2 r} v^{-r} \bmod p$ を満足することを零知識証明を用いて (x_1, x_2, y_1, y_2, r) を秘密としたまま検証者装置に証明する手段を備えることを特徴とする暗号文検証装置。

[CLAIM 29]

A cryptogram verification apparatus, in which in the cryptogram verification apparatus of Claim 28, when V is not equal to 1, (X, Y, V) , with respect to $a(x_1, x_2, y_1, y_2, r)$.

Use zero knowledge proof for satisfying $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, and $V = u_1^{x_1 r + c y_1 r} u_2^{x_2 r + c y_2 r} v^{-r} \bmod p$.

It has means to prove to a verification person apparatus making secret (x_1, x_2, y_1, y_2, r) .

【請求項 30】

請求項 29 の暗号文検証装置において、

g, h は g を底とする h の離散対数が未知であるような G_q の元であって、乱数 r, a_1, a_2, b_1, b_2 を生成する手段と、
 $R = g^r h^a \bmod p$, $RX_1 = R^{x_1} h^{a_1} \bmod p$, $RX_2 = R^{x_2} h^{a_2} \bmod p$, $RY_1 = R^{y_1} h^{b_1} \bmod p$, $RY_2 = R^{y_2} h^{b_2} \bmod p$ なる $R, RX_1, RX_2, RY_1, RY_2$ を公開する手段と、

[CLAIM 30]

A cryptogram verification apparatus, in which in the cryptogram verification apparatus of Claim 29, g and h are under G_q whose discrete logarithm of h which uses g as a bottom is unknown, comprised such that means to form random numbers r, a_1, a_2, b_1 , and b_2 , means to exhibit $R, RX_1, RX_2, RY_1, RY_2$ used as $R = g^r h^a \bmod p$, $RX_1 = R^{x_1} h^{a_1} \bmod p$, $RX_2 = R^{x_2} h^{a_2} \bmod p$, $RY_1 = R^{y_1} h^{b_1} \bmod p$, $RY_2 = R^{y_2} h^{b_2} \bmod p$,

$(X, Y, V, R, RX_1, RX_2, RY_1, RY_2)$ がある

To $(x_1, x_2, y_1, y_2, r, a, a_1, a_2, b_1, b_2)$ with $(X, Y, V, R, RX_1, RX_2, RY_1, RY_2)$, $x = g_1^{x_1} g_2^{x_2} \bmod p$,

$(x_1, x_2, y_1, y_2, r, a, a_1, a_2, b_1, b_2)$ に対して、
 $X = g^{x_1} g^{x_2} \bmod p$, $Y = g^{y_1} g^{y_2} \bmod p$, $V = u^{x_1 r + c y_1 r} u^{x_2 r + c y_2 r} v^{-r} \bmod p$, $R = g^r h^a \bmod p$, $RX_1 = R^{x_1} h^{a_1} \bmod p$, $RX_2 = R^{x_2} h^{a_2} \bmod p$, $RY_1 = R^{y_1} h^{b_1} \bmod p$, $RY_2 = R^{y_2} h^{b_2} \bmod p$ なる関係式を満たすことを零知識証明によって証明する手段とを備えることを特徴とする暗号文検証装置。

$y = g^{y_1} g^{y_2} \bmod p$, $v = u^{x_1 r + c y_1 r} u^{x_2 r + c y_2 r} v^{-r} \bmod p$, $r = g^r h^a \bmod p$, $RX_1 = R^{x_1} h^{a_1} \bmod p$, $RX_2 = R^{x_2} h^{a_2} \bmod p$, $RY_1 = R^{y_1} h^{b_1} \bmod p$, $RY_2 = R^{y_2} h^{b_2} \bmod p$

Means to prove filling the relation used as this by zero knowledge proof

Are provided.

【請求項 31】

請求項 28 の暗号文検証装置において、

n 人の復号者を $P_1 \sim P_n$ とし、

w を $\bmod q$ での 1 の n 乗根とし、 w_j を $w^{j-1} \bmod q$ とし、 $1 < j < n$ において $w_j \neq 1$ を満たすものとし、各復号者 P_j に値 w_j を割り当て、

$(x_1, x_2, y_1, y_2, z) \in \mathbb{Z}_q^5$ を秘密鍵とし、 $X = g^{x_1} g^{x_2} \bmod p$, $Y = g^{y_1} g^{y_2} \bmod p$, $Z = g^{z} \bmod p$ を公開鍵とし、

復号者 P_j の秘密鍵 $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ は、 $3 \leq t < n$ を満たすしきい値 t の秘密分散法により (x_1, x_2, y_1, y_2, z) を分散

[CLAIM 31]

A cryptogram verification apparatus, in which in the cryptogram verification apparatus of Claim 28, it sets n persons' decoding person to P_1 - P_n , let w be n root of 1 in $\bmod q$, it makes w_j into $w^{j-1} \bmod q$, in $1 < j < n$, it shall fill $w_j \neq 1$.

It assigns each decoding person P_j a value w_j , (x_1, x_2, y_1, y_2, z)

Let $(\text{element of}) \mathbb{Z}_q^5$ be a secret key, let $X = g^{x_1} g^{x_2} \bmod p$, $Y = g^{y_1} g^{y_2} \bmod p$, and $Z = g^z \bmod p$ be public key,

Let the decoding person's P_j secret key $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ be the secret value corresponding to a value w_j acquired by dispersing (x_1, x_2, y_1, y_2, z) with the secret dispersion method of threshold-value t which fills $3 \leq t < n$, let $X_j = g^{x_{1j}}$

して得られる、値 w_j に対応する秘密値とし、

$$X_j = g_1^{x_{1j}} g_2^{x_{2j}} \bmod p,$$

$$Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p,$$

$$Z_j = g_1^{z_j} \bmod p \text{ なる } (X_j,$$

$Y_j, Z_j)$ を復号者 P_j の公開鍵とし、

各々の復号者装置間には、安全な通信路があるものとし、また、各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路を利用できるものとし、

乱数 $r \in \mathbb{Z}_q$ をしきい値 t の秘密分散法により分散して、値 w_j に対応する秘密値 r_j を得る手段と、

rx_1, rx_2, ry_1, ry_2 をそれぞれしきい値 t の秘密分散法により分散して、値 w_j に対応する秘密値 $x_{1j}', x_{2j}', y_{1j}', y_{2j}'$ を分散乗算法によって計算して得る手段と、

受信した暗号文について、 $c = H(u_1, u_2)$ を計算する手段と、 $V_j = u_1^{x_{1j}'+cy_{1j}'} u_2^{x_{2j}'+cy_{2j}'} v^{-r_j} \bmod p$ を計算する手段と、

放送型通信路により、 V_j を他の全ての復号者装置へ送信する手段と、

(V_1, \dots, V_n) の指数部が BCH 符号のコードワードであることを確認する手段と、

$g_2^{x_{2j}} \bmod p$, $Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p$, and $Z_j = g_1^{z_j} \bmod p$ be the decoding person's P_j public key (X_j, Y_j, Z_j) , a safe communication channel shall be between each decoding person apparatus.

Moreover, that each decoding person apparatus receives the content with all the members' same other decoding person apparatus shall utilize the broadcast type communication channel guaranteed.

It disperses random-number r (element of) \mathbb{Z}_q with the secret dispersion method of threshold-value t , means to acquire the secret value r_j corresponding to a value w_j ,

It each disperses rx_1, rx_2, ry_1 , and ry_2 with the secret dispersion method of threshold-value t , means which it acquires by calculating secret value $x_{1j}', x_{2j}', y_{1j}'$, and y_{2j}' by the distributed multiplying method, means to calculate $c = H(u_1, u_2)$ about the cryptogram which received, means to calculate $V_j = u_1^{x_{1j}'+cy_{1j}'} u_2^{x_{2j}'+cy_{2j}'} v^{-r_j} \bmod p$, means to transmit V_j to all other decoding person apparatus according to a broadcast type communication channel, means to check that the index part of (V_1, \dots, V_n) is the coding word of a BCH code,

指数部に対する秘密復元手順により V を復元する手段と、復元した値 V が 1 に等しいことを確認することによって暗号文の正当性を検証する手段と、を備えることを特徴とする暗号文検証装置。

Means to decompress V with the secret decompression procedure with respect to an index part, means to verify the correctness of a cryptogram by checking that the decompressed value V is equal to 1

Are provided.

【請求項 3 2】

請求項 3 1 の暗号文検証装置において、

しきい値 t を、 $2 \leq t < n$ を満たすものとし、

(V_1, \dots, V_n) の指数部が BCH 符号のコードワードであることを確認する代わりに、 V_j が $u_1^{x1j'+cy1j'} u_2^{x2j'+cy2j'} v^{-rj} \bmod p$ の正しい計算結果であることを $x1j', x2j', y1j', y2j', rj$ に関する情報を漏らすことなく、零知識証明によって他の復号者に対し証明する手段を備えることを特徴とする暗号文検証装置。

【CLAIM 32】

In the cryptogram verification apparatus of Claim 31, it shall fill $2 \leq t < n$ for threshold-value t .

It has means to prove to another decoding person by zero knowledge proof, without V_j leaking the information concerning [that it is the correct calculation result of $u_1^{x1j'+cy1j'} u_2^{x2j'+cy2j'} v^{-rj} \bmod p$, and] $x1j', x2j', y1j', y2j'$, and rj instead of checking that the index part of (V_1, \dots, V_n) is the coding word of a BCH code.

The cryptogram verification apparatus characterized by the above-mentioned.

【請求項 3 3】

請求項 3 1 の暗号文検証装置において、

(V_1, \dots, V_n) が BCH 符号のコードワードでない場合に、 V_j が $u_1^{x1j'+cy1j'} u_2^{x2j'+cy2j'} v^{-rj} \bmod p$ の計算結果であることを $x1j', x2j', y1j', y2j', rj$ に関する情報を漏らすことなく、零知

【CLAIM 33】

In the cryptogram verification apparatus of Claim 31, means to prove to another decoding person by zero knowledge proof without leaking the information concerning [that V_j is the calculation result of $u_1^{x1j'+cy1j'} u_2^{x2j'+cy2j'} v^{-rj} \bmod p$, and] $x1j', x2j', y1j', y2j'$, and rj when (V_1, \dots, V_n) are not the coding words of a BCH code, it specifies the decoding person P_j who failed in the proof with a deviation person, a deviation

識証明によって他の復号者に証明する手段と、
その証明に失敗した復号者 P_j を逸脱者と特定し、逸脱者の秘密値 $x_{1j'}$, $x_{2j'}$, $y_{1j'}$, $y_{2j'}$, r_j を秘密値回復手順を用いて復元する手段とを備えることを特徴とする暗号文検証装置。

person's secret value $x_{1j'}$, $x_{2j'}$, $y_{1j'}$, $y_{2j'}$, means to decompress r_j using a secret value recovery procedure

Are provided.

The cryptogram verification apparatus characterized by the above-mentioned.

【発明の詳細な説明】

[DETAILED DESCRIPTION OF THE INVENTION]

【0001】

[0001]

【発明の属する技術分野】

この発明は、電気通信システムで通信を行う場合に、通信内容を秘匿し、かつ復号内容を公開した場合にも復号者の秘密鍵に関する情報が漏れることがない安全な暗号方法に関し、特に、暗号文の正当性を復号者が検証する暗号文検証方法及びそのプログラム記録媒体、に関する。

[TECHNICAL FIELD OF THE INVENTION]

This invention relates to the safe cryptographic method from which the information about a decoding person's secret key does not leak, also when the content of communication is kept secret when communicating by a telecommunication system, and the content of decoding is exhibited.

Specifically, it is related with the cryptogram verification method that a decoding person verifies the correctness of a cryptogram, and its program recording medium.

【0002】

[0002]

【従来技術】

選択平文攻撃に強い暗号系においては、暗号文の送信者が元の平文を知っていることを復号者が何らかの方法で検証する。C

[PRIOR ART]

In a code type strong against a choice plaintext attack, a decoding person verifies that the transmitting party of a cryptogram knows original plaintext by a certain method.

r a m e r - S h o u p 暗号 Cramer-Shoup code, paper R.Cramer and
 は、論文 R.Cramer and V.Shoup:"A
 V.Shoup: "A practical public key Practical public key
 cryptosystem provablysecure Cryptosystem provablysecure
 against adaptive chosen Against adaptive chosen
 ciphertext attack", Advances It proposed by ciphertext attack", Advances in
 in Cryptology-CRYPTO'98, Cryptology-CRYPTO'98 and LNCS 1462,
 LNCS 1462, Springer-Verlag, Springer-Verlag, pp.13-25, and 1998, it is the
 pp.13-25, 1998 で提案された、 public-key cryptographic method which can
 汎用一方向性ハッシュ関数の存 prove that it is strong to an adaptive choice
 在および、Diffie-Hellman 判定問 cryptogram attack under assumption which is
 題の困難性という広く信じられ called a presence of a general purpose
 ている仮定の下で、適応的選択 unidirectional hash function and the difficulty of
 暗号文攻撃に強いことが証明で a Diffie-Hellman evaluation problem, and which
 きる公開鍵暗号方法である。 is believed widely.
 Cramer-Shoup 暗号は一つの公 A Cramer-Shoup code is a cryptographic
 開鍵に対応する一つの秘密鍵を method supposing the decoding person of one
 持つ一人の復号者を想定した暗 person with one secret key corresponding to
 号方法である。 one public key.

【0003】

すでに一復号者の場合に適応的
 選択暗号文攻撃に強いことが知
 られている Cramer-Shoup 暗号
 方法では、まず、大きな素数 p 、
 q を、 q が $p-1$ を割り切るよ
 うに選び、乗法群 Z_p の位数 q
 の部分群 G_q の元 g_1, g_2 を
 用いて、秘密鍵を $(x_1, x_2,$
 $y_1, y_2, z) \in Z_q^5$ 公開
 鍵を $X = g_1^{x_1} g_2^{x_2} \bmod p$,
 $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $Z =$
 $g_1^z \bmod p$ とする。平文 $m \in$
 G_q に対する暗号文 E は $(u_1,$
 $u_2, v, e)$ より成り、正し
 く作成された暗号文はある乱数

[0003]

With the Cramer-Shoup cryptographic method
 with which it is already known in the case of the
 1 decoding person that it is strong to an
 adaptive choice cryptogram attack
 First, it chooses the big prime numbers p and q
 so that q may give a clear-cut solution to $p-1$,
 and it uses the origin g_1 and g_2 of the partial
 group G_q of the digit q of multiplicative group
 Z_p , it is (element of) $(x_1, x_2, y_1, y_2, z) \in Z_q^5$
 public key about a secret key, $X = g_1^{x_1} g_2^{x_2} \bmod p$
 It is referred to as $Y = g_1^{y_1} g_2^{y_2} \bmod p$ and $Z = g_1^z$
 $\bmod p$.
 The cryptogram E with respect to plaintext
 m (element of) G_q constitutes of (u_1, u_2, v, e) ,
 and the cryptogram made correctly satisfies

r に対して $u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $c = H(u_1, u_2)$, $v = X^r Y^{cr} \bmod p$, $e = mZ^r \bmod p$ を満足する。この暗号文を受信した復号者は、まず、 $c = H(u_1, u_2)$ を計算し、暗号文が検証式 $u_1^{x_1+cy_1} u_2^{x_2+cy_2} \equiv v \pmod{p}$ を満たすか否かを検証し、満たさない場合にはその暗号文の復号を拒否し、満たす場合には、 $m = e / u_1^z \bmod p$ を計算し、平文 m を得る。

【0004】

上記検証式により、復号者は、暗号文の制作者が元の平文 m を知っていることを確認することができる。検証式を満たさない不正な暗号文に対しては復号を拒否するので、攻撃者は何れの有用な情報も得られない。しかしながら、この暗号文検証方法では、検証の結果復号を拒否する場合に、第三者に対して検証した暗号文が不正であったこと、すなわち、 $V \equiv u_1^{x_1+cy_1} u_2^{x_2+cy_2} \pmod{p}$ として、 $V \neq v \pmod{p}$ とならないことを、 V に関する情報を何ら情報を漏らすことなく証明するのは現実的には困難である。

【0005】

さらに、ElGamal 暗号などでしばしば行われるように、

$u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $c = H(u_1, u_2)$, $v = X^r Y^{cr} \bmod p$, and $e = mZ^r \bmod p$ to a certain random number r .

The decoding person who received this cryptogram calculates $c = H(u_1, u_2)$ first, it verifies whether a cryptogram fills verification type $u_1^{x_1+cy_1} u_2^{x_2+cy_2} \equiv v \pmod{p}$, when not filling, it refuses decoding of the cryptogram, it calculates $m = e / u_1^z \bmod p$, when filling, it obtains Plaintext m .

[0004]

By the above-mentioned verification type, a decoding person can check that the maker of a cryptogram knows original plaintext m .

To the irregular cryptogram which does not fill a verification type, it refuses decoding, therefore, as for neither of the useful information, an aggressor is obtained.

However, when refusing decoding by this cryptogram verification method as a result of verification, it is actually difficult to prove the information concerning [not becoming $V \equiv v \pmod{p}$ and] V , without leaking information in any way as the cryptogram verified to the third person having been illegitimate \pmod{p} , i.e., $V \equiv u_1^{x_1+cy_1} u_2^{x_2+cy_2} \pmod{p}$.

[0005]

Furthermore, the thing for which secret dispersion disperses a corresponding secret

一つの公開鍵に対して、対応する秘密鍵を秘密分散により複数の部分秘密鍵に分散し、複数の復号者にこれを保持させることにより、しきい値を越える人数の復号者が協力したときのみ暗号文を復号できるようにするしきい値付き復号を適用する場合、この暗号復号方法において検証式を満たさないような不正な暗号文に対して、検証式の左辺 $u_1^{x_1+cy_1} u_2^{x_2+cy_2}$ の計算結果 V が複数の復号者に知れてしまうため、攻撃者と結託した復号者が存在した場合に、攻撃者に情報が漏洩してしまい、選択暗号文攻撃への安全性を保つことはできない。

【0006】

しきい値付き復号方法については、例えば、論文 V.Shoup and R.Gennaro: "Securing threshold cryptosystems against chosen ciphertext attack", Advances in Cryptology-EUROCRYPT '98, LNCS 1403, Springer-Verlag, pp.1-16,1998 で提案された方式は、適応的選択暗号文攻撃に強いことがランダムオラクルの存在という仮定の下で示されている。

【0007】

しかしながら、ランダムオラクル

key to two or more partial secret keys to one public key, and it maintains this to two or more decoding persons so that it may often be performed by the ElGamal code etc., to an irregular cryptogram which does not fill a verification type in this code decoding method when the decoding person of the number which exceeds a threshold value cooperates and it applies decoding with the threshold value which enables it to decode a cryptogram, since the calculation result V of left-side $u_1^{x_1+cy_1} u_2^{x_2+cy_2}$ of a verification type becomes known to two or more decoding persons, when the decoding person who conspired with the aggressor exists, information is revealed to an aggressor and it cannot maintain the safety to a choice cryptogram attack.

[0006]

About the decoding method with a threshold value

For example, paper V.Shoup and R.Gennaro :

"Securing threshold

Cryptosystems against

Chosen ciphertext attack

", Advances in Cryptology-EUROCRYPT '98 and LNCS 1403, Springer-Verlag, and pp.1- 16 and 1998 Proposed system, it is shown under assumption called a presence of a random oracle that it is strong to an adaptive choice cryptogram attack.

[0007]

However, assumption called a random oracle is

ルという仮定は、極めて非現実的であり、ランダムオラクルを通常の衝突困難と考えられるハッシュ関数等に置き換えて使用した場合には、その安全性について何の保証も得ることができない。

very unreal.

When a random oracle is replaced and used for the hash function considered that the usual collision is difficult, it can obtain no guarantee about the safety.

【0008】

[0008]

【発明が解決しようとする課題】

[PROBLEM TO BE SOLVED BY THE INVENTION]

この発明の目的は、Cramer-Shoup 暗号において、検証式における値に関する情報を一切漏らすことなく、暗号文の正当性を検証でき、また検証式の値が正当でないことを示している場合に、その値が正しく作成されたものであることを、零知識証明によって第三者に証明することが、更に複数の復号者が協力して検証する場合に、復号者中に不正者がいたとしても、検証式の値が復号者にも漏洩することがない暗号文検証方法、そのプログラム記録媒体、及びその装置を提供することにある。

It sets the objective of this invention to a Cramer-Shoup code, it can verify the correctness of a cryptogram, without leaking the information about the value in a verification type entirely, moreover, the thing for which the value is correctly made when it is shown that the value of a verification type is not rightful, proving for a third person by zero knowledge proof

Furthermore, when two or more decoding persons cooperate and verify, also as there having been an irregular person in a decoding person, the value of a verification type is providing the cryptogram verification method which it does not reveal to a decoding person, either, its program recording medium, and its apparatus.

【0009】

[0009]

【課題を解決するための手段】

[MEANS TO SOLVE THE PROBLEM]

Cramer-Shoup 暗号における復号時の検証式の値を、復号者の誰もがその値を知り得ない乱数

It carries out the power of the value of the verification type at the time of decoding in a Cramer-Shoup code with the random number

によってべき乗し、そのべき乗した結果が1となるか否かを検証することによって暗号文の正当性を検証する。この乱数でべき乗するという計算を分散計算により、全計算者の協力で行うことによって、検証式を満たさない場合にも、べき乗する前の検証式の値はどの復号者にも漏洩することはない、つまり正当でない場合は、計算値が1でない値となり、その値が乱数でべき乗されているから、そのべき乗されている値を示して計算値が1でないこと、即ち正当でないことを示しても、そのべき乗前の値はかくされ、情報が漏れるおそれはない。

【0010】

n 人の復号者を $P_1 \sim P_n$ とし、各復号者 P_j ($j = 1, 2, \dots, n$) は固有の公開値 w_j を持つものとする。 $(x_1, x_2, y_1, y_2, z) \in \mathbb{Z}_{q^5}$ をしきい値 t の秘密分散法により分散し、値 w_j に対応する秘密値 $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ を復号者 P_j の秘密鍵とする。

【0011】

また、 $X_j = g_1^{x_{1j}} g_2^{x_{2j}} \bmod p$, $Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p$, $Z_j = g_1^{z_j} \bmod p$ なる $(X$

with which everyone of a decoding person cannot know the value, and verifies the correctness of a cryptogram by verifying whether the result of having carried out the power is set to 1.

Also when not filling a verification type by performing calculation of carrying out a power by these random numbers, by cooperation of all accountants by distributed calculation, it reveals to no decoding person, that is, the value of the verification type before carrying out a power turns into a value whose calculated value is not 1, when not rightful, the power of the value is carried out by the random numbers, therefore Even if the value by which the power is carried out is shown and it is shown that a calculated value is not 1, i.e., are not rightful, the value in front of the power is hidden, there is no risk that information may leak.

[0010]

It sets n persons' decoding person to $P_1 \sim P_n$, each decoding person P_j ($j = 1, 2, \dots, n$) shall have the inherent open value w_j .

(x_1, x_2, y_1, y_2, z)

It disperses (element of) \mathbb{Z}_{q^5} with the secret dispersion method of threshold-value t , let the secret value $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ corresponding to a value w_j be the decoding person's P_j secret key.

[0011]

Moreover, let (X_j, Y_j, Z_j) which becomes $X_j = g_1^{x_{1j}} g_2^{x_{2j}} \bmod p$, $Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p$, $Z_j = g_1^{z_j} \bmod p$ Be the decoding person's P_j public key.

j , Y_j , Z_j) を復号者 P_j の公開鍵とする。 $X = g^{x_1} g^{x_2} \bmod p$, $Y = g^{y_1} g^{y_2} \bmod p$, $Z = g^{z_1} \bmod p$ なる (X, Y, Z) を暗号化に用いる公開鍵とする。各々の復号者装置間は、安全な通信路で接続されており、各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路を利用できるものとする。

【0012】

$E = (u_1, u_2, v, e)$ を Cramer-Shoup 暗号方法により暗号化された平文 m の暗号文とする。復号者装置は、協力して分散乱数生成手順を実行し、復号者 P_j の装置は秘密値 r_j を得る。ここで、 r_j は乱数 $r \in \mathbb{Z}_q$ をしきい値 t の秘密分散法により分散した場合の、値 w_j に対応する秘密値であり、任意の $t+1$ 個の秘密値から、秘密復号手順により、 r を回復できるような値である。また、分散乱数生成手順の性質から、各復号者装置は r の値を知ることができず、 r は 0 以上 q 未満のランダムな整数となる。

【0013】

Let $X = g^{x_1} g^{x_2} \bmod p$, $Y = g^{y_1} g^{y_2} \bmod p$, and $Z = g^{z_1} \bmod p$ be the public key which it uses for encryption (X, Y, Z) .

It shall connect by the safe communication channel between each decoding person apparatus, and each decoding person apparatus shall utilize the broadcast type communication channel it is guaranteed to be to receive the content with all the members' same other decoding person apparatus.

[0012]

Let $E = (u_1, u_2, v, e)$ be the cryptogram of plaintext m enciphered by the Cramer-Shoup cryptographic method.

A decoding person apparatus performs a distributed random-number generation procedure in cooperation, and the decoding person's P_j apparatus acquires the secret value r_j .

Here, r_j is a secret value corresponding to the value w_j at the time of dispersing random-number r (element of) \mathbb{Z}_q with the secret dispersion method of threshold-value t .

It is the value which can recover r with a secret decoding procedure from the secret values of $t+1$ piece as desired.

Moreover, each decoding person apparatus cannot know the value of r , but r becomes the random integer of 0 or more and under q from the characteristic of a distributed random-number generation procedure.

[0013]

Eを受信した各復号者 P_j の装置は、 $c = H(u_1, u_2)$ および $V_j = (u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-1})^{rj} \bmod p$ を計算する。更に、 V_j をしきい値 $2t$ の検証可能秘密分散法により分散し、値 w_k ($k = 1, 2, \dots, n$ 、 $k \neq j$) に対応する秘密値 V_{jk} を各復号者 P_k の装置に安全な通信路を介して送信する。他の全ての復号者装置から V_{jk} を受信した後、復号者 P_k の装置は V_k を放送型通信路を介して他の全ての復号者装置へ送信する。各復号者装置は受信した各 V_k が正しい値であることを V_{kj} を用いて検証する。

【0014】

正しいと確認された V_k のうち $2t+1$ 個を選択し、指数部、つまり $x1k+cy1k$ 、 $x2k+cy2k$ に対する秘密復元手順により復元した値 V が 1 に等しいか否かを調べる。等しくないならば他の組み合わせで同様に秘密復元手順を繰り返し、全ての $2t+1$ 個の組み合わせについていずれも復元値が 1 に等しくないならば、復号を拒否して停止する。

【0015】

各復号者装置が上記手順に従って計算した場合、 $2t+1$ 個以

The apparatus of each decoding person P_j who received E are $c = H(u_1, u_2)$ and $V_j = (u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-1})^{rj} \bmod p$.

Furthermore, it disperses V_j with a threshold value of $2t$ verifiable secret dispersion method, and transmits the secret value V_{jk} corresponding to a value w_k ($k = 1, 2, \dots, n$, $k \neq j$) through a communication channel safe for each decoding person's P_k apparatus.

After receiving V_{jk} from all other decoding person apparatus, the decoding person's P_k apparatus transmits V_k to etc. of all decoding person apparatus through a broadcast type communication channel.

It verifies using V_{kj} that each decoding person apparatus is the value with each correct V_k which received.

[0014]

If correct, it will choose $2t+1$ piece among checked $V_k(s)$, and it examines whether the value V decompressed by the index part, i.e., the secret decompression procedure with respect to $x1k+cy1k, x2k+cy2k$, is equal to 1.

These

If not equal

It repeats a secret decompression procedure similarly in other combination, and about all $2t+1$ piece combination, if the decompression value is not all equal to 1, it will refuse decoding and will stop.

[0015]

When each decoding person apparatus calculates according to the above-mentioned

上の任意の正しい V_k から、指数部に対する秘密鍵復元手順により、 $V = (u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$ なる V を復元することができる。ここで、 V が p を法として 1 と合同でないならば、Cramer-Shoup 法における本来の検証式 $u_1^{x_1+cy_1} u_2^{x_2+cy_2}$ の値も v と合同ではない。一方、 V が 1 と合同となる場合は、本来の検証式が v と合同であるか、または、乱数 r が 0 であるかのいずれかである。しかしながら、分散乱数生成手順で生成した乱数 r が 0 となる確率は $1/q$ であり、十分小さいので無視する事ができる。従って、 V が 1 と合同である場合には、本来の検証式は v と合同であると見なすことができる。

【0016】

ここで、不正を働く復号者が最大 t 人いると仮定する。この t 人は、(1) 不正な暗号文 E に対する検証式の値 V が 1 となるようにする、または (2) 正当な暗号文 E に対する検証式の値 V が 1 とならないようにする、の二通りの目的で上記手順から逸脱する場合があります。まず、(1) の目的を成功させるためには、ある $2t+1$ 個の V_k か

procedure, from the correct $V_k(s)$ as desired more than $2t+1$ piece, the secret-key decompression procedure with respect to an index part, $v = (u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$.)

Here, v should make p a method

If in cooperation with 1, also the value of original verification type $u_1^{x_1+cy_1} u_2^{x_2+cy_2}$ in Cramer-Shoup method

In cooperation with v .

When V becomes in cooperation with 1 on the other hand, whether an original verification type is in cooperation with v , or

Or whether a random number r is 0, it is either of this.

However, the probabilities that the random number r formed in the distributed random-number generation procedure will be set to 0 are $1/q$.

Since it is small enough, it can ignore.

Therefore, when V is in cooperation with 1, it can consider in cooperation with an original verification type v .

[0016]

Here, it assumes that there are a maximum of t decoding persons who act irregularity.

These t persons, (1)

It makes it the value V of the verification type with respect to the irregular cryptogram E set to 1.

Or

(2)

It keeps the value V of the verification type with respect to the rightful cryptogram E from being set to 1.

ら復元される V の値が 1 となるようにしなければならない。しかしながら、不正者装置を含めた全ての復号者装置は他の復号者装置が出す V_k の値を知る前に、自分の V_k の値を検証可能秘密分散方法によって分散しなければならず、他の復号者装置の V_k の値を知ってから自装置の V_k の値を変更することはできないので、他の復号者装置の V_k に関する予想が当たった場合のみ不正な復号者は (1) の目的を達成することができる。予想が当たる確率は $1/q$ であり、十分小さいので無視することができる。次に、(2) の場合に関しては、不正な復号者装置が、どのような不正な値 V_k を送信したとしても、不正者は高々 t 人であり、他の $2t+1$ 人の装置は正しい値を送信しているので、少なくとも 1 通りは、全て正しい値の $2t+1$ 個の V_k から成る集合を取ることができ、そのような集合から $V=1$ が復元される。

【0017】

情報の漏洩については、 V が 1 でない場合、どのような $u_1^{x_1+cy_1} u_2^{x_2+cy_2}$ の値に対しても、

It can deviate from the above-mentioned procedure for two kinds of these objective.

First

In order to let the objective of (1) successful, you have to make it the value of V decompressed from certain $2t+1$ piece V_k set to 1.

However, all decoding person apparatus including an irregular person apparatus are before getting to know the value of V_k which another decoding person apparatus takes out, since the value of V_k of a self-apparatus cannot be altered after having to disperse the value of one's V_k with a verifiable secret dispersion method and getting to know the value of V_k of another decoding person apparatus, only when the anticipation about V_k of another decoding person apparatus comes true, an irregular decoding person can attain the objective of (1). The probabilities that anticipation will come true are $1/q$.

Since it is small enough, it can ignore.

Next, even if an irregular decoding person apparatus transmits what kind of illegitimate value V_k about the case of (2), an irregular person is at most t persons.

Other $2t+1$ person apparatus have transmitted the correct value, therefore, all the at least 1 kinds can take the ensemble which constitutes of $2t+1$ piece V_k of the correct value, and $V=1$ is decompressed from such an ensemble.

[0017]

About leakage of information, when V is not 1, to the value of what kind of $u_1^{x_1+cy_1} u_2^{x_2+cy_2}$, it is as follows.

$V = (u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \pmod p$ を満たす r の値が一つ
 定まるので、 $(u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})$ の値が r でランダム
 化され、このランダム化された
 値を示しても、 r でランダム化
 される前の値は漏れない、つま
 り上記検証方法では、 $u_1^{x_1+cy_1}$
 $u_2^{x_2+cy_2}$ に関する情報は一切
 漏れない。

【0018】

以上より、この発明によれば、
 不正を働く復号者が全復号者の
 $1/3$ 未満ならば、秘密鍵に関
 する情報を一切漏らすことな
 く、複数復号者の協力によって
 本来の Cramer-Shoup 暗号方法
 の検証式と同等の検証式を計算
 することが可能であり、よって、
 適応的選択暗号文攻撃に強い、
 複数復号者の暗号復号装置を構
 成する事ができる。

【0019】

以上の手法は復号者が n 人いる
 場合に、各復号者装置は、全て
 の復号者装置から受信した n 個
 の検証用データ (V_1, \dots, V_n)
 に対して、 $2t+1$ 個のデ
 ータを取りだし、ある検証式を
 満足するか否かを検証する。満
 足しない場合は、この検証を n
 個に対して取り得る全ての $2t$
 $+1$ 個の組み合わせに対して行
 う。そのため、検証式を満足し

$V = (\text{one value of } r \text{ which fills } u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \pmod p$ becomes settled)

Therefore, the randomizing of the value of
 $(u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})$ is carried out by r , even if
 this value by which the randomizing was carried
 out is shown, the value before a randomizing is
 carried out by r does not leak, that is, the
 information about $u_1^{x_1+cy_1} u_2^{x_2+cy_2}$ does not leak
 at all by the above-mentioned verification
 method.

[0018]

As mentioned above, without leaking the
 information about a secret key entirely, if the
 decoding person who acts irregularity according
 to this invention is under all decoding persons'
 $1/3$, by cooperation of two or more decoding
 person, it can calculate a verification type
 equivalent to the verification type of an original
 Cramer-Shoup cryptographic method, and,
 therefore, can comprise two or more decoding
 person's code decoder strong against an
 adaptive choice cryptogram attack.

[0019]

When n decoding persons are in the above
 approach, to n data for verification (V_1, \dots, V_n)
 which received each decoding person
 apparatus from all decoding person apparatus,
 it takes out $2t+1$ piece data, it verifies whether it
 satisfies a certain verification type.

When not satisfied, it performs this verification
 to all the $2t+1$ piece combination that can be
 taken to n pieces.

Therefore, when not satisfying a verification
 type, it has the disadvantage that computational

ない場合には、復号者の数 n に対して、計算量が指数的に増加するという欠点を持つ。

【0020】

この発明の別の観点によれば、複数の復号者による暗号復号方法において、多数の復号者に対しても効率的に計算が実行でき、また、 $1/3$ 以上の復号者が不正を行っても回復可能であるような、適応的選択暗号文攻撃に強い暗号の暗号文検証方法およびそのプログラム記録媒体を提供する。即ちこの発明の別の観点によれば、まず、復号者の数に対する計算量を低減する手段として、零知識証明によってその結果の正当性を各復号者装置に証明させることによって不正者を特定し、正当なデータのみを用いて暗号文の検証を行う。そうすることによって、復号者の数 n に比例した計算量で検証を行うことが可能である。しかし、この際用いる零知識証明は通信量が多いため、不正がほとんど起こらない場合には効率が悪く、各復号者装置の計算結果が BCH 符号のコードワードとなるように各復号者の固有の公開値を定め、計算結果がコードワードであることを受信者装置が検証し、コードワードでない場合にのみ零知識証明を実行することによって、正しい暗

complexity increases exponentially, to several n of a decoding person.

[0020]

According to another viewpoint of this invention, in the code decoding method by two or more decoding persons, it provides the cryptogram verification method and its program recording medium of a code strong against the adaptive choice cryptogram attack which can be recovered even if it can perform calculation efficiently also to many decoding people and the decoding person who is more than $1/3$ performs irregularity.

That is, as means to reduce the computational complexity with respect to the number of decoding persons, by letting each decoding person apparatus prove the correctness of that result by zero knowledge proof, it specifies an irregular person and, according to another viewpoint of this invention, performs verification of a cryptogram first only using rightful data.

By doing so, it can perform verification by the computational complexity proportional to several n of a decoding person.

However, in this case, since there are many amounts of communication, the zero knowledge proof to be used is, efficiency is bad when irregularity hardly happens.

When the correct cryptogram is received by setting each decoding person's inherent open value that the calculation result of each decoding person apparatus constitutes the coding word of a BCH code, and a receiving-party apparatus verifying that a

号文を受信した場合には、通信量を抑えたまま効率的な計算を行うことが可能となる。

calculation result is the coding word, and performing zero knowledge proof only when it is not the coding word, it becomes that it is possible to perform efficient calculation, with the amount of communication restrained.

【0021】

この方法に因れば、許容できる不正者の数は、 $3t+1 > n$ を満たす t 人までであり、より許容度の高い安全なシステムが望まれる場合には不適當である。また、不正者が $1/3$ 以上 $1/2$ 未満の場合に対応する手段として、不正者が特定された場合に、他の復号者装置が協力してその不正な復号者が持つ分散秘密鍵を算出し、公開することによって、だれもがその不正な復号者に代わって正しい結果を計算することができるようにすることにより、課題を解決する。

[0021]

If based on this method, the number of irregular persons which can be accepted will be to t persons who fill $3t+1 > n$.

It is unsuitable when a safe system with a higher tolerance is desired.

Moreover, it is as means corresponding to the case where irregular persons are $1/3-1/2$, another decoding person apparatus computes the distributed secret key which the irregular decoding person has in cooperation with the case where an irregular person is specified, by opening to the public, although it also becomes bored, it solves a problem by enabling it to calculate the correct result instead of the irregular decoding person.

【0022】

具体的な手段は以下の通りである。 n 人の復号者を $P_1 \sim P_n$ とし、各復号者 P_j に対し、固有の公開値 w_j を割り振る。 $3t < n$ を満たすしきい値 t を定める。 $(x_1, x_2, y_1, y_2, z) \in Z_{q^5}$ をしきい値 t の秘密分散法により分散し、値 w_j に対応する秘密値 $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ を復号者 P_j の秘密鍵とする。

[0022]

The detailed means are as follows.

It sets n persons' decoding person to P_1-P_n , and assigns the inherent open value w_j to each decoding person P_j .

It defines threshold-value t which fills $3t < n$.

(x_1, x_2, y_1, y_2, z)

It disperses (element of) Z_{q^5} with the secret dispersion method of threshold-value t , and let the secret value $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ corresponding to a value w_j be the decoding person's P_j secret key.

【0023】

また、 $X_j = g^{1^{x1j}} g^{2^{x2j}} \bmod p$, $Y_j = g^{1^{y1j}} g^{2^{y2j}} \bmod p$, $Z_j = g^{1^{zj}} \bmod p$ なる (X_j, Y_j, Z_j) を復号者 P_j の公開鍵とする。 $X = g^{1^{x1}} g^{2^{x2}} \bmod p$, $Y = g^{1^{y1}} g^{2^{y2}} \bmod p$, $Z = g^{1^z} \bmod p$ なる (X, Y, Z) を暗号化に用いる公開鍵とする。各々の復号者装置間は、安全な通信路で接続されており、各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路を利用できるものとする。

【0024】

$E = (u_1, u_2, v, e)$ を Cramer-Shoup 暗号方法により暗号化された平文 m の暗号文とする。復号者装置は、協力して分散乱数生成手順を実行し、復号者 P_j の装置は秘密値 r_j を得る。ここで、 r_j は乱数 $r \in \mathbb{Z}_q$ をしきい値 t の秘密分散法により分散した場合の、値 w_j に対応する秘密値であり、任意の $t+1$ 個の秘密値から、秘密復号手順により、 r を回復できるような値である。また、分散乱数生成手順の性質から、各復号者は r の値を知ることができず、 r は 0 以上 q 未満のランダムな整数となる。

[0023]

Moreover, let $X_j = g^{1^{x1j}} g^{2^{x2j}} \bmod p$, $Y_j = g^{1^{y1j}} g^{2^{y2j}} \bmod p$, and $Z_j = g^{1^{zj}} \bmod p$ be the decoding person's P_j public key (X_j, Y_j, Z_j) .

Let $X = g^{1^{x1}} g^{2^{x2}} \bmod p$, $Y = g^{1^{y1}} g^{2^{y2}} \bmod p$, and $Z = g^{1^z} \bmod p$ be the public key which it uses for encryption (X, Y, Z) .

It shall connect by the safe communication channel between each decoding person apparatus, and each decoding person apparatus shall utilize the broadcast type communication channel it is guaranteed to be to receive the content with all the members' same other decoding person apparatus.

[0024]

Let $E = (u_1, u_2, v, e)$ be the cryptogram of plaintext m enciphered by the Cramer-Shoup cryptographic method.

A decoding person apparatus performs a distributed random-number generation procedure in cooperation, and the decoding person's P_j apparatus acquires the secret value r_j .

Here, r_j is a secret value corresponding to the value w_j at the time of dispersing random-number r (element of) \mathbb{Z}_q with the secret dispersion method of threshold-value t .

It is the value which can recover r with a secret decoding procedure from the secret values of $t+1$ piece as desired.

Moreover, each decoding person cannot know the value of r , but r becomes the random integer of 0 or more and under q from the characteristic

of a distributed random-number generation procedure.

【0025】

次に、全復号者装置は協力して分散乗算手段を実行し、各復号者 P_j の装置は秘密値 $x_{1j'}$, $x_{2j'}$, $y_{1j'}$, $y_{2j'}$ を得る。ここで、秘密値 $x_{1j'}$ は、乱数 r と秘密鍵 x_1 の積をしきい値 t の秘密分散法により分散して得られる値であり、任意の $t+1$ 人の復号者が持つ $x_{1j'}$ から、 $r \cdot x_1 \pmod{q}$ を復号することが可能である。秘密値 $x_{2j'}$, $y_{1j'}$, $y_{2j'}$ についても同様に、それぞれ任意の $t+1$ 個の値から、 $r \cdot x_2 \pmod{q}$, $r \cdot y_1 \pmod{q}$, $r \cdot y_2 \pmod{q}$ を復元することができる。

【0026】

E を受信した各復号者 P_j 装置は、 $c = H(u_1, u_2)$ および $V_j = u_1^{x_{1j'} + cy_{1j'}} u_2^{x_{2j'} + cy_{2j'}} v^{-r_j} \pmod{p}$ を計算し、放送型通信路を通じて他の全ての復号者装置へ V_j を送信する。次に、各復号者装置は、 (V_1, \dots, V_n) の指数部が BCH 符号のコードワードであることを確認する。 (V_1, \dots, V_n) の指数部が BCH 符号のコードワードでなく、正しくないことが判明し

[0025]

Next, all decoding person apparatus cooperate and perform distributed multiplication means, each decoding person's P_j apparatus obtains secret value $x_{1j'}, x_{2j'}, y_{1j'}, y_{2j'}$.

Here, secret value $x_{1j'}$ is a value obtained by dispersing the product of a random number r and a secret key x_1 with the secret dispersion method of threshold-value t .

It can decode $x_{1j'}$ to $r \cdot x_1 \pmod{q}$ which $t+1$ person's decoding persons as desired have.

It can decompress $r \cdot x_2 \pmod{q}$, $r \cdot y_1 \pmod{q}$, and $r \cdot y_2 \pmod{q}$ from the values of $t+1$ piece respectively as desired similarly about secret value $x_{2j'}$, $y_{1j'}$, and $y_{2j'}$.

[0026]

Each decoding person P_j apparatus which received E , it calculates $c = H(u_1, u_2)$ and $V_j = u_1^{x_{1j'} + cy_{1j'}} u_2^{x_{2j'} + cy_{2j'}} v^{-r_j} \pmod{p}$, it transmits V_j to all other decoding person apparatus through a broadcast type communication channel.

Next, each decoding person apparatus checks that the index part of (V_1, \dots, V_n) is the coding word of a BCH code.

The index part of (V_1, \dots, V_n) is not the coding word of a BCH code, when it becomes clear that it is not correct, it is each decoding person's P_j apparatus, it proves to another decoding

た場合、各復号者 P_j の装置は、 V_j が $u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-rj} \bmod p$ の計算結果であることを $x1j'$, $x2j'$, $y1j'$, $y2j'$, rj に関する情報を漏らすことなく、零知識証明によって他の復号者に証明する。

【0027】

証明に失敗した復号者 P_j は不正者であると見なされ、その不正者である逸脱者の秘密値 $x1j'$, $x2j'$, $y1j'$, $y2j'$, rj を他の復号者装置が秘密値回復手順を用いて回復し、正しい V_j の値を公開する。公開された正しい V_j の値を含めて、正しい (V_1, \dots, V_n) を得る。 (V_1, \dots, V_n) の指数部が正しいこと、コードワードであることを確認した後、指数部に対する秘密復元手順により、値 V を復元する。各復号者装置は V が 1 に等しいか否かを調べ、等しくないならば復号を拒否して停止する。

【0028】

等しいならば、各復号者 P_j の装置は $D_j = u_1^{zj} \bmod p$ を計算し、放送型通信路により他の全ての復号者装置へ送信する。 D_j を受信した各復号者装置は (D_1, \dots, D_n) に対して、 (V_1, \dots, V_n) に対して行

person by zero knowledge proof, without leaking the information concerning [that V_j is the calculation result of $u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-rj} \bmod p$, and] $x1j', x2j', y1j', y2j', rj$.

[0027]

It considers that the decoding person P_j who failed in proof is an irregular person, another decoding person apparatus recovers secret value $x1j', x2j', y1j', y2j', rj$ of the deviation person who is the irregular person using a secret value recovery procedure, and it exhibits the correct value of V_j .

It includes the exhibited correct value of V_j , it obtains correct (V_1, \dots, V_n) .

After the index part of (V_1, \dots, V_n) checks the correct thing and that it is the coding word, it decompresses a value V with the secret decompression procedure with respect to an index part.

Each decoding person apparatus

It examines whether V is equal to 1, if not equal, it will refuse decoding and will stop.

[0028]

If these etc. come to be by carrying out, each decoding person's P_j apparatus

It calculates $D_j = u_1^{zj} \bmod p$, it transmits to all other decoding person apparatus according to a broadcast type communication channel.

When verification of the coding word similar to having carried out to (V_1, \dots, V_n) is performed to

ったのと同様のコードワードの検証を行い、不正を検出した場合には同様に零知識証明を行って不正者を特定し、正しい D_j の値を秘密値回復手順を用いて回復する。

【0029】

各復号者装置は、正しい(D_1, \dots, D_n)から、指数部に対する秘密復元手順によって $D = u_1^2 \bmod p$ を復元し、 $m = e / D \bmod p$ を計算してメッセージ m を復号する。各復号者装置が上記手順に従って計算した場合、 $2t+1$ 個以上の任意の正しい V_k から、指数部に対する秘密鍵復元手順により、 $V = (u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$ なる V を復元することができる。ここで、 V が p を法として1と合同でないならば、Cramer-Shoup法における本来の検証式 $u_1^{x_1+cy_1} u_2^{x_2+cy_2}$ の値も v と合同ではない。一方、 V が1と合同となる場合は、本来の検証式が v と合同であるか、または、乱数 r が0であるかのいずれかである。しかしながら、分散乱数生成手順で生成した乱数 r が0となる確率は $1/q$ であり、十分小さいので無視する事ができる。従って、 V が1と合同である場合には、本来の検証式は v と合同であると見なすことができる。

(D_1, \dots, D_n) and irregularity is detected, each decoding person apparatus which received D_j performs zero knowledge proof similarly, specifies an irregular person, and recovers the correct value of D_j using a secret value recovery procedure.

[0029]

From it being correct (D_1, \dots, D_n), with the secret decompression procedure with respect to an index part, each decoding person apparatus decompresses $D = u_1^2 \bmod p$, calculates $m = e / D \bmod p$, and decodes Message m .

When each decoding person apparatus calculates according to the above-mentioned procedure, from the correct $V_k(s)$ as desired more than $2t+1$ piece, the secret-key decompression procedure with respect to an index part, it can decompress V used as $V = (u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$.

Here, if V makes p a method.

And is not in cooperation with 1, also the value of original verification type $u_1^{x_1+cy_1} u_2^{x_2+cy_2}$ in Cramer-Shoup method

In cooperation with v .

On the other hand, when V becomes in cooperation with 1, whether in cooperation with an original verification type v , or

Whether a random number r is 0.

It is either of this.

However, the probabilities that the random number r formed in the distributed random-number generation procedure will be set to 0 are $1/q$.

Since it is small enough, it can ignore.

Therefore, when V is in cooperation with 1, it

can consider in cooperation with an original verification type v .

【0030】

ここで、不正を働く復号者が最大 t 人いると仮定する。この t 人は、(1) 不正な暗号文 E に対する検証式の値 V が 1 となるようにする、または (2) 正当な暗号文 E に対する検証式の値 V が 1 とならないようにする、の二通りの目的で上記手順から逸脱する場合があります。しかしながら、全ての復号者装置の出力は BCH 符号のコードワード検査によって検証されるため、不正な値が存在する場合は、不正な値が全体の $1/3$ 未満ならば、その存在を検知することができる。そのような場合には、各々の復号者は零知識証明により出力値の正しさを証明するので、不正な値を出力した不正者は証明に失敗し、排除される。

【0031】

情報の漏洩については、 V が 1 でない場合、どのような $u_1^{x_1+cy_1} u_2^{x_2+cy_2}$ の値に対しても、 $V = (u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$ を満たす r の値が一つ定まるので、上記検証方法では、 $u_1^{x_1+cy_1} u_2^{x_2+cy_2}$ に関する情

[0030]

Here, it assumes that there are a maximum of t decoding persons who act irregularity.

These t persons, (1)

It makes it the value V of the verification type with respect to the irregular cryptogram E set to 1.

Or

(2)

It keeps the value V of the verification type with respect to the rightful cryptogram E from being set to 1.

It can deviate from the above-mentioned procedure for two kinds of these objective.

However, the output of all decoding person apparatus can detect the presence, if an illegitimate value is under whole $1/3$ when an illegitimate value exists since it is verified by the coding word inspection of a BCH code.

In such a case, each decoding person proves the rightness of an output value by zero knowledge proof, therefore, the irregular person who outputted the illegitimate value fails in proof, it is eliminated.

[0031]

About leakage of information

When V is not 1, to the value of what kind of $u_1^{x_1+cy_1} u_2^{x_2+cy_2}$, it is as follows.

$V = (\text{one value of } r \text{ which satisfies } u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p \text{ becomes settled})$

Therefore, by the above-mentioned verification method, the information about $u_1^{x_1+cy_1} u_2^{x_2+cy_2}$

報は一切漏れない。以上より、この発明によれば、不正を働く復号者が全復号者の $1/3$ 未満ならば、秘密鍵に関する情報を一切漏らすことなく、複数復号者の協力によって本来の Cramer-Shoup 暗号方法の検証式と同等の検証式を計算することが可能であり、よって、適応的選択暗号文攻撃に強い、複数復号者の暗号復号方法を構成する事ができる。

【0032】

一方、上記手段において、BCH符号のコードワード検査を行わず、常に零知識証明を実行して不正者を特定し、他の復号者が協力してその不正な復号者が持つ分散秘密鍵を算出し、公開することによって、だれもがその不正な復号者に代わって正しい結果を計算することができるので、 $1/2$ 未満の不正者に対応することができる（零知識証明が正しいことは多数決で決定するため、少なくとも $1/2$ の復号者は正しくなければならない）。

【0033】**【発明の実施の形態】****実施例 1**

以下に、この発明の第一の実施例である暗号文検証方法について

does not leak at all.

As mentioned above, without leaking the information about a secret key entirely, if the decoding person who acts irregularity according to this invention is under all decoding persons' $1/3$, by cooperation of two or more decoding person, it can calculate a verification type equivalent to the verification type of an original Cramer-Shoup cryptographic method, and, therefore, can comprise two or more decoding person's code decoding method strong against an adaptive choice cryptogram attack.

[0032]

On the other hand, for the above-mentioned means, it does not conduct the coding word inspection of a BCH code, it always performs zero knowledge proof and specifies an irregular person, it computes the distributed secret key which another decoding person cooperates and the irregular decoding person has, it opens to the public, although it also becomes bored, instead of the irregular decoding person, the correct result is calculable, therefore, it can respond to the irregular person of under $1/2$ (in order to decide by majority that zero knowledge proof is correct, the decoding person of $1/2$ at least must be correct).

[0033]**[EMBODIMENT OF THE INVENTION]****Example 1**

Below, it demonstrates the cryptogram verification method which is the first Example of

て説明する。図 1 に示すように暗号文作成者装置 11 で作成された暗号文は復号者装置 12 で復号される。復号者装置 12 で、正しい暗号文でないと、勝手に復号拒否することを避けるため、検証者装置 13 で、復号拒否が妥当なものであるか否かを検証する。

【0034】

いま大きな素数 p , q があり、 q は $p-1$ を割り切るものとする。 G_q の元 g_1 , g_2 をランダムに選択する。 $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $Z = g_1^z \bmod p$ を暗号化手順に用いる公開鍵とする。ここで、 $(x_1, x_2, y_1, y_2, z) \in \mathbb{Z}_q^5$ とする。公開鍵は公開パラメータめとして p , q , g_1 , g_2 と共に公開されているものとする。また秘密鍵は復号者装置のメモリ上に格納されているものとする。

【0035】

X , Y , Z を公開鍵とした Cramer-Shoup 暗号方法により暗号化された平文 m の暗号文 $E = (u_1, u_2, v, e)$ を図 2 に示すように受信した後 (S1)、復号者装置は、乱数 r を生成し (S2)、 $c = H(u_1, u_2)$ および $V = (u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$).

this invention.

The cryptogram made with the cryptogram maker apparatus 11 as shown in FIG. 1 is decoded with the decoding person apparatus 12.

If it is not the correct cryptogram with the decoding person apparatus 12, in order to avoid carrying out decoding refusal voluntarily, it verifies whether decoding refusal is appropriate with the verification person apparatus 13.

[0034]

There are big prime numbers p and q now.

Q shall give a clear-cut solution to $p-1$.

It chooses the origin g_1 and g_2 of G_q at random.

Let $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, and $Z = g_1^z \bmod p$ be the public key which it uses for an encryption procedure.

Here, it considers it as (x_1, x_2, y_1, y_2, z) (element of \mathbb{Z}_q^5).

Public key shall be exhibited with p , q , g_1 , and g_2 as an open parameter.

Moreover, the secret key shall be stored on the memory of a decoding person apparatus.

[0035]

After, receiving cryptogram $E = (u_1, u_2, v, e)$ of plaintext m enciphered by the Cramer-Shoup cryptographic method which used X , and Y and Z as public key as shown in FIG. 2, (S1) and a decoding person apparatus form a random number r , and they are (S2), $c = H(u_1, u_2)$, and $V = ((S3) \text{ which calculates } u_1^{x_1+cy_1} u_2^{x_2+cy_2} v^{-1})^r \bmod p$).

$x_2 + cy_2 v^{-1})^r \bmod p$ を計算する (S3)。V が 1 ならば、この暗号文を合格とし (S4)、復号計算を行う (S5)。

【0036】

V が 1 でないならば不合格とする。第三者へ不合格であることを証明するため、ビットコミットメント関数 $BC()$ を用いて、 $BC(r)$ を公開する。このビットコミットメント関数には、たとえば、Pedersen によるものがある。即ち、乱数 s を生成し、 $BC(r, s) := g^r h^s \bmod p$ と計算する。ここで g, h は g を底とする h の離散対数が未知であるような G_q の元である。

【0037】

その後、 $BC(r, s)$ を構成する r と、公開鍵 X, Y を構成する x_1, x_2, y_1, y_2 を用いて $(u_1^{x_1 + cy_1} u_2^{x_2 + cy_2} v^{-1})^r \bmod p$ なる計算を行った結果が V であることを、 r, x_1, x_2, y_1, y_2 に関する秘密を漏らさずに、零知識証明で第三者へ証明する (S6)。この零知識証明は、以下の手順で行う。

【0038】

以下では、 g, h を、 g を底とする h の離散対数が未知であるような G_q の元とする。復号者

If V becomes one, it will consider this cryptogram as a pass and will perform (S4) and decoding calculation (S5).

[0036]

If V is not 1, it will consider it as a rejection.

In order to prove that it is a rejection to a third person, it uses bit commitment function $BC()$, it exhibits $BC(r)$.

There are some which are depended on Pedersen in this bit commitment function, for example.

That is, it forms a random number s , it calculates with $BC(r, s) := g^r h^s \bmod p$.

G and h are here under G_q whose discrete logarithm of h which uses g as a bottom is unknown.

[0037]

After that, r which comprises $BC(r, s)$, it comprises public-key X, Y .

Use x_1, x_2, y_1, y_2 .

The result of having performed calculation used as $(u_1^{x_1 + cy_1} u_2^{x_2 + cy_2} v^{-1})^r \bmod p$ is V , it proves to a third person by zero knowledge proof, without leaking the secret about r, x_1, x_2, y_1, y_2 (S6).

The following procedures perform this zero knowledge proof.

[0038]

Below, it carries out g and h the origin of G_q whose discrete logarithm of h which uses g as a bottom is unknown.

装置は、乱数 a , a_1 , a_2 , b_1 , b_2 を Z_q より選択し、

$$R = g^r h^a \bmod p$$

$$RX1 = R^{x1} h^{a1} \bmod p$$

$$RX2 = R^{x2} h^{a2} \bmod p$$

$$RY1 = R^{y1} h^{b1} \bmod p$$

$$RY2 = R^{y2} h^{b2} \bmod p$$

なる R , $RX1$, $RX2$, $RY1$, $RY2$ を検証者装置へ送付する。

【0039】

さらに、復号者装置は乱数 w_0 を Z_q よりランダムに選択し、

$$K = g, L = g^{w_0} \bmod p$$

を検証者装置へ送付する。検証者装置は、 e_0 および e_1 を Z_q よりランダムに選択して

$$B = K^{e_0} L^{e_1} \bmod p$$

を計算して B を復号者装置へ送付する。

【0040】

復号者装置は乱数 $w_1 \sim w_{18}$ を Z_q よりランダムに選択し、

$$T_1 = g_1^{w_1} g_2^{w_2} \bmod p$$

$$T_2 = g_1^{w_3} g_2^{w_4} \bmod p$$

$$T_3 = g^{w_5} g^{w_6} \bmod p$$

$$T_4 = R^{w_1} h^{w_7} \bmod p$$

$$T_5 = R^{w_2} h^{w_8} \bmod p$$

$$T_6 = R^{w_3} h^{w_9} \bmod p$$

$$T_7 = R^{w_4} h^{w_{10}} \bmod p$$

A decoding person apparatus chooses random numbers a , a_1 , a_2 , b_1 , and b_2 from Z_q , $r = g^r h^a \bmod p$

$$RX1 = R^{x1} h^{a1} \bmod p$$

$$RX2 = R^{x2} h^{a2} \bmod p$$

$$RY1 = R^{y1} h^{b1} \bmod p$$

$$RY2 = R^{y2} h^{b2} \bmod p$$

It sends $R, RX1, RX2, RY1, RY2$ used as this to a verification person apparatus.

[0039]

Furthermore, a decoding person apparatus chooses a random number w_0 from Z_q at random, $k = g$, $L = g^{w_0} \bmod p$

It sends these to a verification person apparatus.

A verification person apparatus chooses e_0 and e_1 from Z_q at random.

$$B = K^{e_0} L^{e_1} \bmod p$$

It calculates these and sends B to a decoding person apparatus.

[0040]

A decoding person apparatus chooses random-number w_1 - w_{18} from Z_q at random, t_1

$$= g_1^{w_1} g_2^{w_2} \bmod p$$

$$T_2 = g_1^{w_3} g_2^{w_4} \bmod p$$

$$T_3 = g^{w_5} g^{w_6} \bmod p$$

$$T_4 = R^{w_1} h^{w_7} \bmod p$$

$$T_5 = R^{w_2} h^{w_8} \bmod p$$

$$T_6 = R^{w_3} h^{w_9} \bmod p$$

$$T_7 = R^{w_4} h^{w_{10}} \bmod p$$

$$T_8 = g^{w_{11}} h^{w_{12}} \bmod p$$

$$T_9 = g^{w_{13}} h^{w_{14}} \bmod p$$

$$T_{10} = g^{w_{15}} h^{w_{16}} \bmod p$$

$$T_{11} = g^{w_{17}} h^{w_{18}} \bmod p$$

$$T_8 = g^{w_{11}} h^{w_{12}} \bmod p$$

$$T_9 = g^{w_{13}} h^{w_{14}} \bmod p$$

$$T_{10} = g^{w_{15}} h^{w_{16}} \bmod p$$

$$T_{11} = g^{w_{17}} h^{w_{18}} \bmod p$$

$$T_{12} = u_1^{w_{11}+cw_{15}} u_2^{w_{13}+cw_{17}} v^{-w_5} \bmod p$$

を計算して、検証者装置へ送付する。

$$T_{12} = u_1^{w_{11}+cw_{15}} u_2^{w_{13}+cw_{17}} v^{-w_5} \bmod p$$

It calculates these and sends to a verification person apparatus.

【0041】

検証者装置は、 e_0 , e_1 を復号者装置へ送付する。

復号者装置は、 $B = K^{e_0} L^{e_1} \bmod p$

が成り立つことを確認し、成り立たない場合は証明を中止する。これが成り立つ場合、復号者装置は

$$z_1 = w_1 + e_0 \cdot x_1 \bmod q$$

$$z_2 = w_2 + e_0 \cdot x_2 \bmod q$$

$$z_3 = w_3 + e_0 \cdot y_1 \bmod q$$

$$z_4 = w_4 + e_0 \cdot y_2 \bmod q$$

$$z_5 = w_5 + e_0 \cdot r \bmod q$$

$$z_6 = w_6 + e_0 \cdot a \bmod q$$

$$z_7 = w_7 + e_0 \cdot a_1 \bmod q$$

[0041]

A verification person apparatus sends e_0 and e_1 to a decoding person apparatus.

A decoding person apparatus is $B = K^{e_0} L^{e_1} \bmod p$. It checks that these are formed, it stops proof, when not formed.

When this is formed, it is a decoding person apparatus.

$$Z_1 = w_1 + e_0 \text{ and } x_1 \bmod q$$

$$Z_2 = w_2 + e_0 \text{ and } x_2 \bmod q$$

$$Z_3 = w_3 + e_0 \text{ and } y_1 \bmod q$$

$$Z_4 = w_4 + e_0 \text{ and } y_2 \bmod q$$

$$Z_5 = w_5 + e_0 \text{ and } r \bmod q$$

$$Z_6 = w_6 + e_0 \text{ and } a \bmod q$$

$$Z_7 = w_7 + e_0 \text{ and } a_1 \bmod q$$

$$Z_8 = w_8 + e_0 \text{ and } a_2 \bmod q$$

$$Z_9 = w_9 + e_0 \text{ and } b_1 \bmod q$$

$$z_8 = w_8 + e_0 \cdot a_2 \bmod q$$

q

$$z_9 = w_9 + e_0 \cdot b_1 \bmod q$$

q

$$z_{10} = w_{10} + e_0 \cdot b_2 \bmod q \quad Z_{10} = w_{10} + e_0 \text{ and } b_2 \bmod q$$

q

$$Z_{11} = w_{11} + e_0 \text{ and } r \cdot x_1 \bmod q$$

$$z_{11} = w_{11} + e_0 \cdot r \cdot x_1 \bmod q \quad Z_{12} = w_{12} + e_0 (a \cdot x_1 + a_1) \bmod q$$

mod q

$$Z_{13} = w_{13} + e_0 \text{ and } r \cdot x_2 \bmod q$$

$$z_{12} = w_{12} + e_0 (a \cdot x_1 + a_1) \bmod q$$

$$z_{13} = w_{13} + e_0 \cdot r \cdot x_2$$

mod q

$$z_{14} = w_{14} + e_0 (a \cdot x_2 + a_2) \bmod q \quad Z_{14} = w_{14} + e_0 (a \cdot x_2 + a_2) \bmod q$$

a_2) mod q

$$Z_{15} = w_{15} + e_0 \text{ and } r \cdot y_1 \bmod q$$

$$z_{15} = w_{15} + e_0 \cdot r \cdot y_1 \bmod q \quad Z_{16} = w_{16} + e_0 (a \cdot y_1 + b_1) \bmod q$$

mod q

$$Z_{17} = w_{17} + e_0 \text{ and } r \cdot y_2 \bmod q$$

$$z_{16} = w_{16} + e_0 (a \cdot y_1 + b_1) \bmod q$$

b_1) mod q

$$z_{17} = w_{17} + e_0 \cdot r \cdot y_2$$

mod q

$$z_{18} = w_{18} + e_0 (a \cdot y_2 + b_2) \bmod q \quad Z_{18} = w_{18} + e_0 (a \cdot y_2 + b_2) \bmod q$$

b_2) mod q

It calculates these and sends z1-z18 and w0 to

を計算して z 1 ~ z 1 8 および a verification person apparatus.

w 0 を検証者装置へ送付する。

【0042】

検証者装置は、

$$L = g^{w_0} \bmod p$$

$$g_1^{z_1} g_2^{z_2} = T_1 X^{e_0} \bmod p$$

$$g_1^{z_3} g_2^{z_4} = T_2 Y^{e_0} \bmod p$$

$$g^{z_5} h^{z_6} = T_3 R^{e_0} \bmod p$$

$$R^{z_1} h^{z_7} = T_4 (R X_1)^{e_0} \bmod p$$

[0042]

Verification person apparatus, $l = g^{w_0} \bmod p$

$$G_1^{z_1} g_2^{z_2} = T_1 X^{e_0} \bmod p$$

$$G_1^{z_3} g_2^{z_4} = T_2 Y^{e_0} \bmod p$$

$$G^{z_5} h^{z_6} = T_3 R^{e_0} \bmod p$$

$$R^{z_1} h^{z_7} = T_4 (RX_1)^{e_0} \bmod p$$

$$R^{z2}h^{z8} = T_5 (RX2)^{e0} \bmod p \quad R^{z2}h^{z8} = T_5 (RX2)^{e0} \bmod p$$

$$R^{z3}h^{z9} = T_6 (RY1)^{e0} \bmod p$$

$$R^{z4}h^{z10} = T_7 (RY2)^{e0} \bmod p \quad R^{z4}h^{z10} = T_7 (RY2)^{e0} \bmod p$$

$$G^{z11}h^{z12} = T_8 (RX1)^{e0} \bmod p$$

$$G^{z13}h^{z14} = T_9 (RX2)^{e0} \bmod p$$

$$G^{z15}h^{z16} = T_{10} (RY1)^{e0} \bmod p$$

$$G^{z15}h^{z16} = T_{10} (RY1)^{e0} \bmod p$$

$$G^{z15}h^{z16} = T_{10} (RY1)^{e0} \bmod p$$

$$G^{z17}h^{z18} = T_{11} (RY2)^{e0} \bmod p$$

$$U_1^{z11+cz15} U_2^{z13+cz17} V^{-z5} = T_{12} V^{e0} \bmod p$$

$$U_1^{z11+cz15} U_2^{z13+cz17} V^{-z5} = T_{12} V^{e0} \bmod p$$

$$U_1^{z11+cz15} U_2^{z13+cz17} V^{-z5} = T_{12} V^{e0} \bmod p$$

が成り立つことを検証する。

【0043】

上の証明の原理は、Schnorr 署名と同様であり、復号者装置が V, X, Y, R, RX1, RX2, RY1, RY2 を正しく作成した場合にのみ検証式が成り立つので、一つでも成り立たない場合は検証を失敗とする。

【実施例 2】

以下に、この発明の第二の実施例について説明する。図 3 に示すように暗号作成者装置 11 と復号者 P1 ~ Pn の各装置 12₁ ~ 12_n とは放送型通信路 1

[0043]

The principle of the upper proof is Schnorr. It is the same as that of a signature.

Since a verification type is formed only when a decoding person apparatus makes correctly V, X, and Y, R, RX1, RX2, RY1 and RY2, when at least one is not formed, it considers verification as failure.

[EXAMPLE 2]

Below, it demonstrates the 2nd Example of this invention.

As shown in FIG. 3, the code maker apparatus 11, and each apparatus 12₁-12_n of decoding person P1-Pn are connected to the broadcast

4に接続され、また復号者装置
12₁ ~ 12_nは相互に安全な
通信路15で接続されている。

type communication channel 14, moreover,
decoding person apparatus 12₁ -12_n is
connected by the mutually safe communication
channel 15.

【0044】

いま大きな素数 p , q があり、
 q は $p-1$ を割り切るものとする。
 G_q の元 g_1 , g_2 をランダムに選択する。まず、 n 人の
復号者を $P_1 \sim P_n$ とし、各復号者
 P_j ($j = 1, 2, \dots, n$) に対し、固有の公開値 w_j を割り振る。
 $3 \leq t \leq n$ を満たすしきい値 t を定める。全復号者装置は、しきい値 t の分散乱数生成手順を3回実行し、復号者 P_j の装置は秘密値 $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ を得、これを復号者 P_j の秘密鍵とする。また、 $X_j = g_1^{x_{1j}} g_2^{x_{2j}} \bmod p$, $Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p$, $Z_j = g_1^{z_j} \bmod p$ なる (X_j, Y_j, Z_j) を復号者 P_j の公開鍵とする。さらに、 $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, $Z = g_1^z \bmod p$ を暗号化手順に用いる公開鍵とする。ここで、 $(x_1, x_2, y_1, y_2, z) \in Z_q^5$ は任意の $t+1$ 組の秘密値 $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ から、秘密復元手順により復元される乱数である。このような乱数を生成する分散乱数生成手順には、例えば、

[0044]

There are big prime numbers p and q now.
 Q shall give a clear-cut solution to $p-1$.
It chooses the origin g_1 and g_2 of G_q at random.
First, it sets n persons' decoding person to $P_1 \sim P_n$, to each decoding person P_j ($j = 1, 2, \dots, n$)
It assigns the inherent open value w_j .
It defines threshold-value t which fills $3 \leq t \leq n$.
All decoding person apparatus perform the distributed random-number generation procedure of threshold-value t 3 times, the decoding person's P_j apparatus acquires a secret value $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$, let this be the decoding person's P_j secret key.
Moreover, let $X_j = g_1^{x_{1j}} g_2^{x_{2j}} \bmod p$, $Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p$, and $Z_j = g_1^{z_j} \bmod p$ be the decoding person's P_j public key (X_j, Y_j, Z_j) .
Furthermore, let $X = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = g_1^{y_1} g_2^{y_2} \bmod p$, and $Z = g_1^z \bmod p$ be the public key which it uses for an encryption procedure.
Here, $(x_1, x_2, y_1, y_2, z) \in Z_q^5$ is a random number decompressed by a secret decompression procedure from $t+1$ set of secret values $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ as desired.
There is the method of depending on Pedersen in the number generation procedure of part scattering which forms such a random number, for example.
Below, the distributed random-number

P e d e r s e n による方法がある。以下に、その分散乱数生成手順を示す。

generation procedure is shown.

【 0 0 4 5 】

各々の復号者装置間には、図 3 に示したように安全な通信路 15 があるものとし、また、各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路 14 を利用できるものとする。

S-1) P_j の装置は Z_q 上の二つの多項式 $f(X) = a_0 + a_1X + \dots + a_tX^t$ および $g_j(X) = b_0 + b_1X + \dots + b_tX^t$ をランダムに選択し、各 P_k の装置 ($k = 1, 2, \dots, n, k \neq j$) へ $f_j(w_k)$ および $g_j(w_k)$ を安全な通信路を通じて送信する。

[0045]

As shown in FIG. 3, the safe communication channel 15 shall be between each decoding person apparatus, and each decoding person apparatus shall utilize the broadcast type communication channel 14 it is guaranteed to be to receive the content with all the members' same other decoding person apparatus.

S-1)

The apparatus of P_j chooses two polynomial $f(X) = a_0 + a_1X + \dots + a_tX^t$ and, and $g_j(X) = b_0 + b_1X + \dots + b_tX^t$ on Z_q at random, it transmits $f_j(w_k)$ and $g_j(w_k)$ to each apparatus ($k = \text{except for } 1, 2, \dots, n, \text{ and } k \neq j$) of P_k through a safe communication channel.

【 0 0 4 6 】

S-2) P_j の装置は $i = 1, \dots, t$ に対して $C_{ij} = g_1^{a_{ij}} g_2^{b_{ij}} \bmod p$ を計算し、放送型通信路を通じて他の全ての復号者装置へ送信する。

S-3) 他の全ての復号者装置から C_{ij} を受信した P_k の装置は $w_k^i = w_k^i \bmod q$ として $g_1^{f_j(w_k)} g_2^{g_j(w_k)} = C_{0j}^{w_k^0} \cdot C_{1j}^{w_k^1} \dots C_{tj}^{w_k^t} \bmod p$ が成り立つことを検証する。

[0046]

S-2)

The apparatus of P_j should receive $i = 1, \dots, t$. It calculates $C_{ij} = g_1^{a_{ij}} g_2^{b_{ij}} \bmod p$, it transmits to all other decoding person apparatus through a broadcast type communication channel.

S-3)

The apparatus of P_k which received C_{ij} from all other decoding person apparatus verifies that $g_1^{f_j(w_k)} g_2^{g_j(w_k)} = C_{0j}^{w_k^0} \cdot C_{1j}^{w_k^1} \dots C_{tj}^{w_k^t} \bmod p$ is formed as $w_k^i = w_k^i \bmod q$.

【 0 0 4 7 】

[0047]

S-4) P_k の装置は $x_{1k} =$

$f_1(w_k) + f_2(w_k) + \dots + f_n(w_k) \bmod q$ 、 $x_{2k} = g_1(w_k) + g_2(w_k) + \dots + g_n(w_k) \bmod q$ として分散乱数値 x_{1k} 、 x_{2k} を得る。

S-5) $X = C_{00} \cdot C_{01} \dots C_{0n} \bmod p$ とする。同様に公開鍵 Y 、 Z および各復号者の対応する秘密鍵 y_{1j} 、 y_{2j} 、 z_j も同様に作成する。

【0048】

全復号者装置は、分散乱数生成手順によって、分散された乱数 $r \in Z_q$ を生成し、各復号者 P_j の装置は秘密値 r_j を保持する (図5, S1)。 X 、 Y 、 Z を公開鍵とした Cramer-Shoup 暗号方法により暗号化された平文 m の暗号文 $E = (u_1, u_2, v, e)$ を受信した後 (S2)、各復号者 P_j の装置は、 $c = H(u_1, u_2)$ および $V_j = (u_1^{x_{1j}+cy_{1j}} u_2^{x_{2j}+cy_{2j}} v^{-1})^{r_j} \bmod p$ を計算する (S3)。

【0049】

続いて P_j の装置は V_j をしきい値 $2t$ の検証可能秘密分散法により分散し、値 w_k に対応する秘密値 V_{jk} を各復号者 P_k の装置に安全な通信路を介して送信する (S4)。ここで用いる検証可能秘密分散法には、 P_e

S-4)

The apparatus of P_k obtains distributed random-number value x_{1k}, x_{2k} as $x_{1k} = f_1(w_k) + f_2(w_k) + \dots + f_n(w_k) \bmod q$, $x_{2k} = g_1(w_k) + g_2(w_k) + \dots + g_n(w_k) \bmod q$.

S-5)

It considers it as $X = C_{00} \cdot C_{01} \dots C_{0n} \bmod p$.

It also makes similarly secret-key y_{1j} , y_{2j} , and z_j to which public key Y and Z and each decoding person correspond similarly.

[0048]

All decoding person apparatus form dispersed random-number r (element of) Z_q with a distributed random-number generation procedure, and each decoding person's P_j apparatus maintains the secret value r_j (FIG. 5, S1).

After receiving cryptogram $E = (u_1, u_2, v, e)$ of plaintext m enciphered by the Cramer-Shoup cryptographic method which used X, Y, Z as public key, the apparatus of (S2) and each decoding person P_j are $c = H(u_1, u_2)$ and $V_j = ((S3) \text{ which calculates } u_1^{x_{1j}+cy_{1j}} u_2^{x_{2j}+cy_{2j}} v^{-1})^{r_j} \bmod p$).

[0049]

Then, the apparatus of P_j disperses V_j with a with a threshold value of $2t$ verifiable secret dispersion method, and it transmits the secret value V_{jk} corresponding to a value w_k through a communication channel safe for each decoding person's P_k apparatus (S4).

It can use the method of Pedersen for the

dersenの方法を用いることができる。以下はその手順である。

P-1) 大きな素数 P , Q があり、 Q は $P-1$ を割り切り、また $Q > p$ とする、 g および h は、 $\log_g h$ の値が未知であるような G_Q の元とする。

【0050】

P-2) P_j の装置は Z_Q 上の二つの多項式 $f_j(X) = V_j + a_{1j}X + \dots + a_{tj}X^t$ および $g_j(X) = b_{0j} + b_{1j}X + \dots + b_{tj}X^t$ (ただし $a_{0j} = V_j$ とする) を V_j の部分を除いてランダムに選択し、各 P_k の装置へ $f_j(w_k)$ および $g_j(w_k)$ 、つまり V_{jk} を安全な通信路を通じて送信する。

P-3) P_j の装置は $i = 1, \dots, t$ に対して $C_{ij} = g^{a_{ij}} h^{b_{ij}} \bmod p$ を計算し、放送型通信路を通じて他の全ての復号者装置へ送信する。

【0051】

P-4) C_{ij} を受信した P_k の装置は $w_k i = w_k^i \bmod q$ として $g^{f_j(w_k)} h^{g_j(w_k)} = C_{0j}^{w_k 0} \cdot C_{1j}^{w_k 1} \dots C_{tj}^{w_k t} \bmod p$ が成り立つことを検証する、つまり V_{jk} を検証する (S5)。

P-5) 成り立たない場合、 P_k の装置は「不合格」を放送型通信路を通じて他の全ての復号

verifiable secret dispersion method which it uses here.

The following is the procedure.

P-1) There are big prime numbers P and Q .

G and h which Q gives a clear-cut solution to $P-1$, and it makes into $Q > p$ are the origin of G_Q whose value of $\log_g h$ is unknown.

[0050]

P-2)

The apparatus of P_j

Two polynomial $f_j(X) = V_j + a_{1j}X + \dots + a_{tj}X^t$ and, $g_j(X) = b_{0j} + b_{1j}X + \dots + b_{tj}X^t$ on Z_Q

(However, it is referred to as $a_{0j} = V_j$)

Except for the part of V_j , it chooses this at random, it transmits $f_j(w_k)$ and $g_j(w_k)$, i.e., V_{jk} , to each apparatus of P_k through a safe communication channel.

P-3)

The apparatus of P_j should receive $i = 1, \dots, t$.

It calculates $C_{ij} = g^{a_{ij}} h^{b_{ij}} \bmod p$, it transmits to all other decoding person apparatus through a broadcast type communication channel.

[0051]

The apparatus of P_k which received P-4 C_{ij} verifies that $g^{f_j(w_k)} h^{g_j(w_k)} = C_{0j}^{w_k 0} \cdot C_{1j}^{w_k 1} \dots C_{tj}^{w_k t} \bmod p$ is formed as $w_k i = w_k^i \bmod q$, that is, verifies V_{jk} (S5).

P-5)

When not formed, the apparatus of P_k transmits a "rejection" to all other decoding person apparatus through a broadcast type communication channel.

者装置へ送信する。

【0052】

P-6)「不合格」通知が $t+1$ 個以上である場合、 P_j は不正者と見なされて排除され (S6)、他の全復号者装置は P_j の装置が以前に送信した全ての情報を廃棄する。P-4, 5, 6 のステップは分散秘密値 V_{jk} の検証と、不正者の排除を行う手順であり、全ての復号者装置がデータを送信し終わった後、まとめて不合格リストを公表することで行ってもよい。

[0052]

P-6)

When the notification of a "rejection" is $t+1$ or more pieces, it is regarded as an irregular person, and is eliminated and P_j is (S6), other all decoding person apparatus

The apparatus of P_j aborts all the information transmitted before.

The step of P-s 4, 5, and 6 is the procedure of performing verification of the distributed secret value V_{jk} , and an irregular person's rejection.

After all decoding person apparatus finish transmitting data, it is sufficient to carry out by releasing a rejection list collectively.

【0053】

全復号者装置が上記手順によって V_j を分散した後、各復号者 P_j の装置は、 V_j および b_{0j} を放送型通信路を通じて他の全ての復号者装置へ送信する (S7)。これを受信した各復号者 P_j の装置は、 $C_{0j} = g^{-1} V_j^{b_{0j}} \bmod p$ が成り立つことを確認して V_j を検証する (S8)。成り立たない場合は、前記同様、「不合格」を他の全復号者装置へ通知し、不正者を排除する (S9)。

[0053]

After all decoding person apparatus disperse V_j with the above-mentioned procedure, each decoding person's P_j apparatus, v_j and b_{0j}

It transmits to all other decoding person apparatus through a broadcast type communication channel (S7).

The apparatus of each decoding person P_j who received this checks that $C_{0j} = g^{-1} V_j^{b_{0j}} \bmod p$ is formed, and verifies V_j (S8).

When not formed, it notifies a "rejection" to other all decoding person apparatus like the above, it eliminates an irregular person (S9).

【0054】

正しいと確認された全ての V_k から任意に $2t+1$ 個を選択し (S10)、指数部に対する秘密

[0054]

If correct, it will choose $2t+1$ piece from all checked $V_k(s)$ as desired (S10), and it examines whether the value V decompressed

復元手順により復元した値 V が 1 に等しいか否かを調べる (S11)。指数部に対する秘密復元手順は文献 Cramer, et.al: "A secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology-Eurocrypt'97, LNCS 1233 Springer-Verlag, pp.103-118, 1997 に詳しい。以下に、選択した $2t+1$ 個の V_k のインデックス k の集合を α とした場合の指数部に対する復元手順を示す。指数部の秘密値は Pedersen の検証可能秘密分散法で得られた秘密値であるとする。

【0055】

R-1) まず、Lagrange 補間係数を

【0056】

【数1】

$$\lambda_{j,\alpha} = \prod_{k \in \alpha, k \neq j} j/(j-k)$$

として計算する。

R-2) 次に、

【0057】

with the secret decompression procedure with respect to an index part is equal to 1 (S11).

The secret decompression procedures with respect to an index part are documents. Cramer, et.al: "A secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology-Eurocrypt'97, LNCS 1233 Springer-Verlag, pp.103-118, and 1997 It is detailed.

The decompression procedure with respect to the index part at the time of making into (alpha) an ensemble of the index k of $2t+1$ piece V_k chosen as below is shown.

The secret value of an index part presupposes that it is the secret value acquired with the verifiable secret dispersion method of Pedersen.

[0055]

R-1) IT IS LAGRANGE INTERPOLATION COEFFICIENT FIRST.

[0056]

[EQUATION 1]

It calculates as these.

R-2) NEXT,

[0057]

【数 2】

[EQUATION 2]

$$V = \prod_{j \in \alpha} V_j^{\lambda_j \cdot \alpha} \bmod p$$

を計算する。Vが1でないならば他の $2t+1$ 個の組み合わせで同様に秘密復元手順を繰り返す(S12)。全ての組み合わせについていずれも復元値が1に等しくないならば、不合格を通知して停止する。

It calculates these.

If V is not 1, it will repeat a secret decompression procedure similarly in other $2t+1$ piece combination (S12).

About all combination, if the decompression value is not all equal to 1, it will notify a rejection and will stop.

【0058】

[0058]

一つでも1になる組み合わせがあったならば、この暗号文を合格とする。各復号者 P_j の装置は図4に示すように $D_j = u_1^{z_j} \bmod p$ を計算し(S1)、放送型通信路により他の全ての復号者装置へ送信する(S2)。 D_j を受信した各復号者装置は D_1, \dots, D_n の u_1 を底とする離散対数がBCH符号のコードワードであることを確認し(S4)、コードワードであれば、前述の指数部に対する秘密復元手順により $D = u_1^z \bmod p$ を復元し(S5)、 $m = e / D \bmod p$ を計算してメッセージ m を復号する(S6)。ステップS4でコードワードでなければ、零知識証明により、計算の正しさを証明させ、証明できないものは

If there is combination set to 1 at least one, it will consider this cryptogram as a pass.

As shown in FIG. 4, each decoding person's P_j apparatus calculates $D_j = u_1^{z_j} \bmod p$, and transmits it to all other decoding person apparatus according to (S1) and a broadcast type communication channel (S2).

Each decoding person apparatus which received D_j

By checking that the discrete logarithm which uses u_1 of D_1, \dots, D_n as a bottom is the coding word of a BCH code, if it is (S4) and the coding word, it will decompress $D = u_1^z \bmod p$ with the secret decompression procedure with respect to the above-mentioned index part, it will calculate (S5) and $m = e / D \bmod p$, and will decode Message m (S6).

If it is not the coding word in step S4, it will prove the rightness of calculation by zero knowledge proof.

不正の D_i として廃棄する (S7)。

It aborts the thing which cannot be proved as irregular D_i (S7).

【実施例 3】

以下に、この発明の第三の実施例について説明する。

[EXAMPLE 3]

Below, it demonstrates the 3rd Example of this invention.

【0059】

各々の復号者装置間には、安全な通信路があるものとし、また、各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路を利用できるものとする。大きな素数 p , q があり、 q は $p-1$ を割り切るものとする。 G_q の元 g_1 , g_2 をランダムに選択する。まず、 n 人の復号者を $P_1 \sim P_n$ とし、各復号者 P_j に対し、固有の公開値 w_j を割り振る。 $3 \leq t \leq n$ を満たすしきい値 t を定める。

[0059]

That a safe communication channel shall be between each decoding person apparatus, and each decoding person apparatus receives the content with all the members' same other decoding person apparatus shall utilize the broadcast type communication channel guaranteed.

There are big prime numbers p and q .

Q shall give a clear-cut solution to $p-1$.

It chooses the origin g_1 and g_2 of G_q at random.

First, it sets n persons' decoding person to $P_1 \sim P_n$, and assigns the inherent open value w_j to each decoding person P_j .

It defines threshold-value t which fills $3 \leq t \leq n$.

【0060】

まず、Pedersen による秘密分散方法を示す。まず、 g , h を $\log_g h$ が未知であるような G_q の元とする。秘密値 a_0 , b_0 を分散する分配者 P の装置は、 Z_q 上の t 次の二つの多項式 $f(X) = a_0 + a_1 X + \dots + a_t X^t$, $g(X) = b_0 + b_1 X + \dots + b_t X^t$ を a_0 を除いてランダムに選択し、各受信者 P_j の装置へ $f(w_j)$, $g(w_j)$

[0060]

First, the secret dispersion method by Pedersen is shown.

First, it carries out g and h the origin of G_q whose $\log_g h$ is unknown.

The apparatus of the portioner P who disperses the secret values a_0 and b_0 are the t -th two polynomial $f(X) = a_0 + a_1 X + \dots + a_t X^t$ on Z_q , except for a_0 , it chooses $g(X) = b_0 + b_1 X + \dots + b_t X^t$ at random, and sends $f(w_j)$ and $g(w_j)$ to the apparatus of each receiving party P_j through a safe communication channel.

j) を安全な通信路を通じて送付する。

【0061】

つぎに、各係数のコミット値 E_i を $i = 0, \dots, t$ に対して $E_i = g^{a_i} h^{b_i} \bmod p$ のように計算し、放送型通信路を介して公開する。これらを受信した各 P_j の装置は、 $u_{ji} = w_j^i \bmod q$ として $g^{f(w_j)} h^{g(w_j)} = E_0^{u_{j0}} E_1^{u_{j1}} \dots E_t^{u_{jt}} \bmod p$ が成り立つことを検証する。この $E_0^{u_{j0}} E_1^{u_{j1}} \dots E_t^{u_{jt}} \bmod p$ の値を P_j の分散秘密値に対するコミットメントと呼ぶ。各係数のコミット値が公開されていれば、誰でも、どの P_j の分散秘密値に対するコミットメントも計算することができる。

【0062】

以下では、この秘密分散方法を $Ped(a_0, b_0) [g, h] \rightarrow (a_{0j}, b_{0j}) (E_0, \dots, E_t)$ のように書く。 (a_0, b_0) は分散される秘密情報であり、 (a_{0j}, b_{0j}) は各 P_j の装置が安全な通信路を介して受信する分散秘密値であり、それぞれ $f(w_j), g(w_j)$ に等しい。 (E_0, \dots, E_t) は放送型通信路を通じて公開される、各係数のコミット値である。 $[g, h]$ はコミットを作成する際に用い

[0061]

Next, it calculates the commitment value E_i of each coefficient like $E_i = g^{a_i} h^{b_i} \bmod p$ to $i = 0 \dots, t$, and opens to the public through a broadcast type communication channel.

Each apparatus of P_j which received these verifies that $g^{f(w_j)} h^{g(w_j)} = E_0^{u_{j0}} E_1^{u_{j1}} \dots E_t^{u_{jt}} \bmod p$ is formed as $u_{ji} = w_j^i \bmod q$.

It calls the value of this $E_0^{u_{j0}} E_1^{u_{j1}} \dots E_t^{u_{jt}} \bmod p$ the commitment with respect to the distributed secret value of P_j .

If the commitment value of each coefficient is exhibited, anyone can also calculate the commitment with respect to which distributed secret value of P_j .

[0062]

Below, it is this secret dispersion method.

$Ped(a_0, b_0) [g, h] \rightarrow (a_{0j}, b_{0j}) (E_0, \dots, E_t)$

It writes like these.

(a_0, b_0) are confidential informations dispersed.

(a_{0j}, b_{0j}) are distributed secret values which it receives through a communication channel with each safe apparatus of P_j .

It is equal to $f(w_j)$ and $g(w_j)$ respectively.

(E_0, \dots, E_t) are commitment values of each coefficient exhibited through a broadcast type communication channel.

$[g, h]$

express the bottom which it uses when making a commitment.

る底を表す。上記記法に関して、特に断りがない限り、定数項を除く多項式の係数はランダムに選ぶものとする。

It is related with the above-mentioned account method.

Specifically, as long as there is no notice, it shall choose the coefficient of the polynomial except an absolute term at random.

【0063】

このようにして分散された秘密値から、多項式補間によって元の秘密を回復する場合には、まず、各分散秘密値の保持者は、その値を公開する。公開された (a_{0j}, b_{0j}) 値に対して、 $g^{a_{0j}} h^{b_{0j}} = E_0^{u_{j0}} E_1^{u_{j1}} \dots E_t^{u_{jt}} \bmod p$ が成り立つことを確認する。この式が成り立つような任意の $t+1$ 個の (a_{0j}, b_{0j}) について、そのインデックス j が作る集合を α とする。Lagrange 補間係数を

[0063]

Thus, from the dispersed secret value, when a polynomial interpolation recovers the original secret, the holder of each distributed secret value exhibits the value first.

It checks that $g^{a_{0j}} h^{b_{0j}} = E_0^{u_{j0}} E_1^{u_{j1}} \dots E_t^{u_{jt}} \bmod p$ is formed to the exhibited value (a_{0j}, b_{0j}) .

Let the ensemble which the index j makes be (α) about $t+1$ $(a_{0j}$ as desired, $b_{0j})$ of which this equation consists.

Lagrange interpolation coefficient

【0064】

[0064]

【数3】

[EQUATION 3]

$$\lambda_{i,\alpha} = \prod_{k \in \alpha, k \neq i} i/(i-k) \bmod q$$

とすると、

When it carries out,

【0065】

[0065]

【数4】

[EQUATION 4]

$$\sum_{j \in \alpha} \lambda_{j, \alpha} a_{0j} \bmod q = a_0$$

となり、 a_0 を回復することができる。 b_0 も同様にして回復できる。上記秘密分散方法は、底を一つだけ用いても全く同様に実行することができる。そのような場合は、 $Ped(a_0)$
 $[g] \rightarrow (a_{0j})(E_0, \dots, E_t)$ と書く。

【0066】

この秘密分散方法を利用して、複数人が協調して分散された乱数を生成することができる。まず、 P_i の装置は、乱数 a_i 、 b_i を Z_q より選択し、これを
 $Ped(a_i, b_i)[g, h] \rightarrow (a_{ij}, b_{ij})(E_{i0} \dots, E_{it})$
 のように分散する。 $P_1 \sim P_n$ の全員がこれを実行する。すると、 P_j の装置は、 $(a_{1j}, b_{1j}), \dots, (a_{nj}, b_{nj})$ を安全な通信路から受信し、 $(E_{10}, \dots, E_{1t}), \dots, (E_{n0}, \dots, E_{nt})$ を放送型通信路から受信する。このとき、 P_j の分散秘密値 (x_{1j}, x_{2j}) を、 $x_{1j} = a_{1j} + \dots + a_{nj} \bmod q$ 、 $x_{2j} = b_{1j} + \dots + b_{nj} \bmod q$ とする。この分散秘密値から回復される乱数値 x_1 は、

A these next door, a_0 is recoverable.

B_0 is recoverable similarly.

Even if it uses only one bottom, it can completely perform the above-mentioned secret dispersion method similarly.

In such a case

$Ped(a_0)[g]$ It writes it as $\rightarrow (a_{0j})(E_0 \dots, E_t)$.

[0066]

The random number dispersed in cooperation by two or more persons is generable using this secret dispersion method.

First, the apparatus of P_i chooses random numbers a_i and b_i from Z_q , this

$Ped(a_i, b_i)[g, h] \rightarrow (a_{ij}, b_{ij})(E_{i0} \dots, E_{it})$

It disperses like these.

All the members of $P_1 \sim P_n$ perform this.

Then, the apparatus of P_j receives $(a_{1j}, b_{1j}), \dots, (a_{nj}, b_{nj})$ from a safe communication channel, it receives $(E_{10} \dots, E_{1t}), \dots, (E_{n0} \dots, E_{nt})$ from a broadcast type communication channel.

At this time, it sets the distributed secret value (x_{1j}, x_{2j}) of P_j to $x_{1j} = a_{1j} + \dots + a_{nj} \bmod q$, $x_{2j} = b_{1j} + \dots + b_{nj} \bmod q$.

The random-number value x_1 recovered from this distributed secret value,

【 0 0 6 7 】

[0067]

【数 5】

[EQUATION 5]

$$x_1 = \sum_{j \in \alpha} \lambda_{k, \alpha} x_{1j} = a_1 + \dots + a_n \mod q$$

であり、回復が実行されるまでは、誰にもその値が知られることはない。また、この秘密乱数値を定数とする多項式の k 次の係数のコミット値 EX_k は、 $EX_k = E_{1k} \cdot E_{2k} \cdots E_{nk} \mod p$ となる。特に、 $EX_0 = g^{x_1} h^{x_2} \mod p$ であることに注意。この方法を、分散乱数生成とよび、
 $Rand([a], [b]) [g, h] \rightarrow (a_j, b_j) (E_0, \dots, E_t)$

と書く。 $([a], [b])$ は、生成される乱数値であり、 $[]$ はその値がどの計算者に対しても未知であることを意味する。 $[g, h], (a_j, b_j)$ および (E_0, \dots, E_t) の意味は、前述の秘密分散の記法と同様である。

They are these.

The value is known by nobody until recovery is performed.

Moreover, the commitment value EX_k of the k -th coefficient of the polynomial which makes this secret random-number value a constant constitutes $EX_k = E_{1k} \cdot E_{2k} \cdots E_{nk} \mod p$.

Particularly, it is cautious of it being $EX_0 = g^{x_1} h^{x_2} \mod p$.

It calls this method distributed random-number generation, $rand([a], [b]) [g, h] \rightarrow (a_j, b_j) (E_0, \dots, E_t)$

It writes.

$([a], [b])$ are random-number values formed.

$[]$

means that the value is unknown to every accountant.

The implication of $[g, h], (a_j, b_j)$ and (E_0, \dots, E_t) is the same as that of the account method of above-mentioned secret dispersion.

【 0 0 6 8 】

[0068]

全復号者装置は、しきい値 t の分散乱数生成手順を

$Rand([x_1], [x_2]) [g_1, g_2] \rightarrow (x_{1j}, x_{2j})$

All decoding person apparatus are the distributed random-number generation procedures of threshold-value t .

$Rand([x_1], [x_2]) [g_1, g_2] \rightarrow (x_{1j}, x_{2j}) (EX_0, \dots,$

(EX_0, \dots, EX_t)
 $Rand([y_1], [y_2]) [g_1, g_2] \rightarrow (y_{1j}, y_{2j})$
 (EY_0, \dots, EY_t)
 $Rand([z_1]) [g_1] \rightarrow (z_{1j})$
 (EZ_0, \dots, EZ_t)

$EX_t)$
 $Rand([y_1], [y_2]) [g_1, g_2] \rightarrow (y_{1j}, y_{2j}) (EY_0, \dots, EY_t)$
 $Rand([z_1]) [g_1] \rightarrow (z_{1j}) (EZ_0, \dots, EZ_t)$

のように3回実行し、復号者 P_j は秘密値 $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ を得、これを復号者 P_j の秘密鍵とする。また、 $X_j = g_1^{x_{1j}} g_2^{x_{2j}} \bmod p$, $Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p$, $Z_j = g_1^{z_j} \bmod p$ なる (X_j, Y_j, Z_j) を復号者 P_j の公開鍵とする。さらに、 $X = EX_0 = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = EY_0 = g_1^{y_1} g_2^{y_2} \bmod p$, $Z = EZ_0 = g_1^z \bmod p$ を暗号化手順に用いる公開鍵とする。ここで $(x_1, x_2, y_1, y_2, z) \in Z_q^5$ は任意の $t+1$ 組の秘密値 $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ から、秘密復元手順により復元される乱数である。

It performs 3 times like these, the decoding person P_j acquires a secret value $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$, let this be the decoding person's P_j secret key.

Moreover, let $X_j = g_1^{x_{1j}} g_2^{x_{2j}} \bmod p$, $Y_j = g_1^{y_{1j}} g_2^{y_{2j}} \bmod p$, and $Z_j = g_1^{z_j} \bmod p$ be the decoding person's P_j public key (X_j, Y_j, Z_j) .

Furthermore, let $X = EX_0 = g_1^{x_1} g_2^{x_2} \bmod p$, $Y = EY_0 = g_1^{y_1} g_2^{y_2} \bmod p$, and $Z = EZ_0 = g_1^z \bmod p$ be the public key which it uses for an encryption procedure.

(element of) $(x_1, x_2, y_1, y_2, z) Z_q^5$ is a random number decompressed by a secret decompression procedure from $t+1$ set of secret values $(x_{1j}, x_{2j}, y_{1j}, y_{2j}, z_j)$ as desired here.

【0069】

全復号者装置は、分散乱数生成手順 $Rand([r], [s]) [g_1, g_2] \rightarrow (r_j, s_j) (R_0, \dots, R_t)$ を実行し、分散された乱数 $r \in Z_q$ を生成し、各復号者 P_j の装置は秘密値 r_j, s_j を保持する (図6、S1)。ここで R を $R = R_0 = g_1^r g_2^s \bmod p$

[0069]

All decoding person apparatus perform distributed random-number generation procedure $Rand([r], [s]) [g_1, g_2] \rightarrow (r_j, s_j) (R_0, \dots, R_t)$, it forms dispersed random-number r (element of) Z_q , each decoding person's P_j apparatus maintains the secret values r_j and s_j (FIG. 6, S1).

It makes R into $R = R_0 = g_1^r g_2^s \bmod p$ here.

$r \cdot g^{2^s} \bmod p$ とする。

【0070】

次に、全復号者装置は、分散乗算手段によって秘密値 $x_{1j'}$, $x_{2j'}$, $y_{1j'}$, $y_{2j'}$ を得る (S2)。ここで、秘密値 $x_{1j'}$ は、乱数 r と秘密鍵 x_1 の積をしきい値 t の秘密分散法により分散して得られる値であり、任意の $t+1$ 人の復号者が持つ $x_{1j'}$ から、 $r \cdot x_1 \bmod q$ を復号することが可能である。秘密値 $x_{2j'}$, $y_{1j'}$, $y_{2j'}$ についても同様に、それぞれ任意の $t+1$ 個の値から、 $r \cdot x_2 \bmod q$, $r \cdot y_1 \bmod q$, $r \cdot y_2 \bmod q$ を復元することができる。このような分散乗算手段については、以下のように実行する。

【0071】

復号者 P_j の装置は、
 $Ped(x_{1j}, x_{2j})[g_1, g_2] \rightarrow (x_{1ji}, x_{2ji})$
 $(EX_{j0}, \dots, EX_{jt})$
 を実行する。各 P_j の装置は、
 $R_j = g_1^{r_j} g_2^{s_j} \bmod p$ を計算する。この値 R_j は、 $u_{ji} = w_j^i \bmod q$ として $R_j = R_0^{u_{j0}} R_1^{u_{j1}} \dots R_t^{u_{jt}} \bmod p$ のように計算しても良いので、誰でも計算できることに注意。

【0072】

[0070]

Next, all decoding person apparatus obtain secret value $x_{1j'}$, $x_{2j'}$, $y_{1j'}$, and $y_{2j'}$ by distributed multiplication means (S2).

Here, secret value $x_{1j'}$ is a value obtained by dispersing the product of a random number r and a secret key x_1 with the secret dispersion method of threshold-value t .

From $x_{1j'}$ which $t+1$ person's decoding persons as desired have, it can decode $rx_1 \bmod q$.

It can decompress $rx_2 \bmod q$, $ry_1 \bmod q$, and $ry_2 \bmod q$ from the values of $t+1$ piece respectively as desired similarly about secret value $x_{2j'}$, $y_{1j'}$, and $y_{2j'}$.

About such distributed multiplication means, it performs as follows.

[0071]

The decoding person's P_j apparatus, $ped(x_{1j}, x_{2j})[g_1, g_2] \rightarrow (x_{1ji}, x_{2ji})$ (EX_{j0}, \dots, EX_{jt})

It performs these.

Each apparatus of P_j calculates $R_j = g_1^{r_j} g_2^{s_j} \bmod p$.

Since this value R_j may be calculated like $R_j = R_0^{u_{j0}} R_1^{u_{j1}} \dots R_t^{u_{jt}} \bmod p$ as $u_{ji} = w_j^i \bmod q$, it cautions it about the ability of anyone to calculate.

[0072]

次に、 P_j の装置は、 $Ped(x_{1j}, x_{2j})$ で x_{1j}, x_{2j} を分散するのに用いた多項式をそのまま用いて、 $Ped(x_{1j}, s_{1j}) [R_j, g_2] \rightarrow (x_{1ji}, s_{1ji}) (ERX_{1j0}, \dots, ERX_{1jt})$
 $Ped(x_{2j}, s_{2j}) [R_j, g_2] \rightarrow (x_{2ji}, s_{2ji}) (ERX_{2j0}, \dots, ERX_{2jt})$

を実行する。ただし、 s_{1j}, s_{2j} はランダムに選び、また、これらを定数項とする多項式もランダムに選ぶ。

【0073】

最後に、 P_j の装置は

$Ped(x_{1j} \cdot r_j, x_{1j} \cdot s_j + s_{1j}) [g_1, g_2] \rightarrow (rx_{1ji}, rs_{1ji}) (ERX_{1j0}, \dots, ERX_{1jt})$
 $Ped(x_{2j} \cdot r_j, x_{2j} \cdot s_j + s_{2j}) [g_1, g_2] \rightarrow (rx_{2ji}, rs_{2ji}) (ERX_{2j0}, \dots, ERX_{2jt})$
 とする。

【0074】

上記手順を $P_1 \sim P_n$ の各装置が実行する。 P_i の装置は、受信した分散秘密値の集合 $(rx_{11i}, \dots, rx_{1ni})$ から、Lagrange 補間係数を

【0075】

Next, the polynomial used for dispersing x_{1j} and x_{2j} by $Ped(x_{1j}, x_{2j})$ is used for the apparatus of P_j as it is, and it is $Ped(x_{1j}, s_{1j}) [R_j, g_2] \rightarrow (x_{1ji}, s_{1ji}) (ERX_{1j0}, \dots, ERX_{1jt})$.

$Ped(x_{2j}, s_{2j}) [R_j, g_2] \rightarrow (x_{2ji}, s_{2ji}) (ERX_{2j0}, \dots, ERX_{2jt})$

It performs these.

However, s_{1j} and s_{2j} also choose at random the polynomial which chooses at random and makes these an absolute term.

[0073]

To the last, it is the apparatus of P_j .

$Ped(x_{1j} \cdot r_j, x_{1j} \cdot s_j + s_{1j}) [g_1, g_2] \rightarrow (rx_{1ji}, rs_{1ji}) (ERX_{1j0}, \dots, ERX_{1jt})$

$Ped(x_{2j} \cdot r_j, x_{2j} \cdot s_j + s_{2j}) [g_1, g_2] \rightarrow (rx_{2ji}, rs_{2ji}) (ERX_{2j0}, \dots, ERX_{2jt})$

It carries out.

[0074]

Each apparatus of $P_1 \sim P_n$ performs the above-mentioned procedure.

The apparatus of P_i is the ensemble $(rx_{11i}, \dots, rx_{1ni})$ of a distributed secret value which received to a Lagrange interpolation coefficient.

[0075]

【数 6】

[EQUATION 6]

$\lambda_{j, \alpha} = \prod_{k \in \alpha, k \neq j} j/(j-k)$ として、

$$x_{1j'} = \sum_{j \in \alpha} \lambda_{j, \alpha} r x_{1j} \pmod{q}$$

As $(\lambda_{j, \alpha})_{j \in \alpha} = \text{llk}(\alpha)$, k not equal to $j/(j-k)$,

を計算する。正しい $x_{1j'}$ の
インデックスの集合を β とし、
 $|\beta| \geq t+1$ のとき、

It calculates these.

Let an ensemble of the index of correct $x_{1j'}$ be
(beta), | At the time of (beta)| $\geq t+1$

【0076】

[0076]

【数 7】

[EQUATION 7]

$$\begin{aligned} \sum_{j \in \beta} \lambda_{j, \beta} x_{1j'} &= \sum_{j \in \beta} \{ \lambda_{j, \beta} \sum_{i \in \alpha} \lambda_{i, \alpha} r x_{1i} \} \\ &= \sum_{i \in \alpha} \lambda_{i, \alpha} \{ \sum_{j \in \beta} \lambda_{j, \beta} r x_{1i} \} \\ &= \sum_{i \in \alpha} \lambda_{i, \alpha} r i \cdot x_{1i} = r \cdot x_1 \end{aligned}$$

となり、乗算結果 $r \cdot x_1$ を回復することができるので、 $x_{1j'}$ が $r \cdot x_1$ の t 次の分散秘密値であることが分かる。 $x_{1j'}$ と同様に、 $x_{2j'}$ も計算する。更に、秘密値 $y_{1j'}$, $y_{2j'}$ についても同様に分散乗算手順を実行して計算する。

At these next door, multiplication result $r \cdot x_1$ is recoverable, therefore, it turns out that $x_{1j'}$ is the t -th distributed secret value of $r \cdot x_1$.

It calculates $x_{2j'}$ as well as $x_{1j'}$.

Furthermore, it performs and calculates a distributed multiplication procedure similarly about secret value $y_{1j'}$ and $y_{2j'}$.

【0077】

[0077]

Cramer-Shoup 暗号方法により暗号化された平文 m に対する暗

After receiving cryptogram $E=(u_1, u_2, v, e)$ with respect to plaintext m enciphered by the

号文 $E = (u_1, u_2, v, e)$ を受信した後 (S3)、各復号者 P_j の装置は、 $c = H(u_1, u_2)$ および $V_j = u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-rj} \bmod p$ を計算し (S4)、放送型通信路を通じて他の全ての復号者装置へ V_j を送信する (S5)。次に、各復号者装置は、 (V_1, \dots, V_n) の指数部が BCH 符号のコードワードであることを確認する (S6)。コードワード確認手順は、文献 F.J. MacWilliams: "The Thory of Error Correcting Codes", North-Holland Mathematical Library, pp.201-202 または、M.Ben-Or, S.Goldwasser, A.Wigerson: "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation", 20th ACM Symposium on Theory of Computing, pp.1-10, 1988 に詳しい。以下にコードワード確認手順を示す。

- ・ $w \neq 1$ を $\bmod q$ での 1 の n 乗根とし、 $\xi_{ij} = w^{j(i-1)} \bmod q$ とする。
- ・ $j = 1, \dots, 2t$ の全ての j について

【0078】

【数8】

Cramer-Shoup cryptographic method, the apparatus of (S3) and each decoding person P_j calculates $c = H(u_1, u_2)$ and $V_j = u_1^{x1j+cy1j} u_2^{x2j+cy2j} v^{-rj} \bmod p$. (S4), it transmits V_j to all other decoding person apparatus through a broadcast type communication channel.

(S5).

Next, each decoding person apparatus checks that the index part of (V_1, \dots, V_n) is the coding word of a BCH code.

(S6).

Coding word check procedure, documents

F.J. MACWILLIAMS: "THE THORY OF ERROR CORRECTING CODES", NORTH-HOLLAND MATHEMATICAL LIBRARY, PP.201-202

Or

M.Ben-Or, S.Goldwasser, a.Wigerson:

"Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Comput

It is detailed to ation", 20th ACM Symposium on Theory of Computing", pp.1-10, and 1988.

The coding word check procedure is shown below.

It considers it as n root of 1 in $w^i = 1 \bmod q$, it considers it as $(\xi_{ij})_{ij} = w^{j(i-1)} \bmod q$.

All j of $j=1, \dots, 2t$

[0078]

[EQUATION 8]

$$V_1^{E_1} V_2^{E_2} \dots V_n^{E_n} \bmod p = 1$$

となることを確認する。上記手順により、 (V_1, \dots, V_n) の指数部が正しくないことが判明した場合、各復号者 P_j の装置は、 V_j が $u_1^{x_1j+cy_1j} u_2^{x_2j+cy_2j} v^{-r_j} \bmod p$ の計算結果であることを $x_1j', x_2j', y_1j', y_2j', r_j$ に関する情報を漏らすことなく、零知識証明によって他の復号者装置に証明する (S7)。

【0079】

この零知識証明は、以下のよう
に実行する。ただし、以下の P_j
に対する手順の説明では、全
ての変数に添字 j が付くため、
これを省いて説明する。まず、
 P_j の保持する分散秘密値 $x_1', x_2', y_1', y_2', r$
に対して、 a, a_1, a_2, b_1 をある乱数として

$$\begin{aligned} R &= g_1^{r'} g_2^s \bmod p \\ RX_1 &= ERX_{10} = R^{x_1} g_2^{a_1} \bmod p \\ RX_2 &= ERX_{20} = R^{x_2} g_2^{a_2} \bmod p \end{aligned}$$

$$\begin{aligned} RY_1 &= ERY_{10} = R^{y_1} g_2^{b_1} \bmod p \\ RY_2 &= ERY_{20} = R^{y_2} g_2^{b_2} \bmod p \end{aligned}$$

It checks becoming these.

When it becomes clear with the above-mentioned procedure that the index part of (V_1, \dots, V_n) is not correct, it is each decoding person's P_j apparatus, without it leaks the information concerning that V_j is the calculation result of $u_1^{x_1j+cy_1j} u_2^{x_2j+cy_2j} v^{-r_j} \bmod p$, and $x_1j', x_2j', y_1j', y_2j', r_j$, it proves to another decoding person apparatus by zero knowledge proof (S7).

[0079]

It performs this zero knowledge proof as follows.

However, by explanation of the procedure with respect to following P_j , since Subscript j is attached to all variables, it excludes and demonstrates this.

First, it is to distributed secret value x_1' which P_j maintains, x_2', y_1', y_2' , and r considering a, a_1, a_2 , and b_1 as a certain random number.

$$\begin{aligned} R &= g_1^{r'} g_2^s \bmod p \\ RX_1 &= ERX_{10} = R^{x_1} g_2^{a_1} \bmod p \\ RX_2 &= ERX_{20} = R^{x_2} g_2^{a_2} \bmod p \end{aligned}$$

$$\begin{aligned} RY_1 &= ERY_{10} = R^{y_1} g_2^{b_1} \bmod p \\ RY_2 &= ERY_{20} = R^{y_2} g_2^{b_2} \bmod p \end{aligned}$$

It can acquire the values $R, RX_1, RX_2, RY_1,$

$b^2 \bmod p$

なるコミットメントの値 R , $R X 1$, $R X 2$, $R Y 1$, $R Y 2$ を、分散乱数生成手段および、分散乗算手段で公開された係数のコミット値から、誰にでも得ることができる。

【0080】

P_j は乱数 w_0 を Z_q よりランダムに選択し、

$$K = g, L = g^{w_0} \bmod p$$

を他の復号者装置へ送付する。

他の復号者装置は、協力して $Rand([e_0], [e_1]) [K, L] \rightarrow (e_{0i}, e_{1i}) (Ee_0, \dots, Ee_t)$

を実行し、 $Ee_0 = K^{e_0} L^{e_1} \bmod p$ を P_j の装置へ送付する。

【0081】

P_j の装置は乱数 $w_1 \sim w_{18}$ を Z_q よりランダムに選択し、

$$T_1 = g_1^{w_1} g_2^{w_2} \bmod p$$

$$T_2 = g_1^{w_3} g_2^{w_4} \bmod p$$

$$T_3 = g^{w_5} g^{w_6} \bmod p$$

$$T_4 = R^{w_1} h^{w_7} \bmod p$$

$$T_5 = R^{w_2} h^{w_8} \bmod p$$

$$T_6 = R^{w_3} h^{w_9} \bmod p$$

$$T_7 = R^{w_4} h^{w_{10}} \bmod p$$

$$T_8 = g^{w_{11}} h^{w_{12}} \bmod p$$

$$T_9 = g^{w_{13}} h^{w_{14}} \bmod p$$

$$T_{10} = g^{w_{15}} h^{w_{16}} \bmod p$$

and $RY2$ of the becoming commitment from the commitment value of the coefficient exhibited with distributed random-number generation means and distributed multiplication means to anyone.

[0080]

P_j chooses a random number w_0 from Z_q at random, $k=g$, $L=g^{w_0} \bmod p$

It sends these to another decoding person apparatus.

Another decoding person apparatus cooperates.

$Rand([e_0], [e_1]) [K, L] \rightarrow (e_{0i}, e_{1i}) (Ee_0, \dots, Ee_t)$

It performs these, it sends $Ee_0 = K^{e_0} L^{e_1} \bmod p$ to the apparatus of P_j .

[0081]

The apparatus of P_j chooses random-number $w_1 \sim w_{18}$ from Z_q at random, $t_1 = g_1^{w_1} g_2^{w_2} \bmod p$

$$T_2 = g_1^{w_3} g_2^{w_4} \bmod p$$

$$T_3 = g^{w_5} g^{w_6} \bmod p$$

$$T_4 = R^{w_1} h^{w_7} \bmod p$$

$$T_5 = R^{w_2} h^{w_8} \bmod p$$

$$T_6 = R^{w_3} h^{w_9} \bmod p$$

$$T_7 = R^{w_4} h^{w_{10}} \bmod p$$

$$T_8 = g^{w_{11}} h^{w_{12}} \bmod p$$

$$T_9 = g^{w_{13}} h^{w_{14}} \bmod p$$

$$T_{10} = g^{w_{15}} h^{w_{16}} \bmod p$$

$$T_{11} = g^{w17} h^{w18} \bmod p$$

$$T_{11} = g^{w17} h^{w18} \bmod p$$

$$T_{12} = u_1^{w11+cw15} u_2^{w13+cw17} v^{-w5} \bmod p$$

$$T_{12} = u_1^{w11+cw15} u_2^{w13+cw17} v^{-w5} \bmod p$$

を計算して、他の復号者装置へ送付する。

It calculates these, it sends to another decoding person apparatus.

【0082】

他の復号者装置は分散秘密値を公開して e_0 , e_1 を回復し、 P_j の装置へ送付する。 P_j の装置は、 $E e_0 = K^{e_0} L^{e_1} \bmod p$ が成り立つことを確認し、成り立たない場合は証明を中止する。これが成り立つ場合、 P_j の装置は

$$S_1 = w_1 + e_0 \cdot x_1 \bmod q$$

$$S_2 = w_2 + e_0 \cdot x_2 \bmod q$$

$$S_3 = w_3 + e_0 \cdot y_1 \bmod q$$

$$S_4 = w_4 + e_0 \cdot y_2 \bmod q$$

$$S_5 = w_5 + e_0 \cdot r \bmod q$$

$$S_6 = w_6 + e_0 \cdot a \bmod q$$

$$S_7 = w_7 + e_0 \cdot a_1 \bmod q$$

$$S_8 = w_8 + e_0 \cdot a_2 \bmod q$$

$$S_9 = w_9 + e_0 \cdot b_1 \bmod q$$

$$S_{10} = w_{10} + e_0 \cdot b_2 \bmod q$$

$$S_{11} = w_{11} + e_0 \cdot r \cdot x_1 \bmod q$$

$$S_{12} = w_{12} + e_0 \cdot (a \cdot x_1 + a_1) \bmod q$$

$$S_{13} = w_{13} + e_0 \cdot r \cdot x_2 \bmod q$$

$$S_{14} = w_{14} + e_0 \cdot (a \cdot x_2 + a_2) \bmod q$$

$$S_{15} = w_{15} + e_0 \cdot r \cdot y_1 \bmod q$$

$$S_{16} = w_{16} + e_0 \cdot r \cdot y_2 \bmod q$$

$$S_{17} = w_{17} + e_0 \cdot r \cdot y_3 \bmod q$$

$$S_{18} = w_{18} + e_0 \cdot r \cdot y_4 \bmod q$$

$$S_{19} = w_{19} + e_0 \cdot r \cdot y_5 \bmod q$$

$$S_{20} = w_{20} + e_0 \cdot r \cdot y_6 \bmod q$$

$$S_{21} = w_{21} + e_0 \cdot r \cdot y_7 \bmod q$$

$$S_{22} = w_{22} + e_0 \cdot r \cdot y_8 \bmod q$$

$$S_{23} = w_{23} + e_0 \cdot r \cdot y_9 \bmod q$$

$$S_{24} = w_{24} + e_0 \cdot r \cdot y_{10} \bmod q$$

[0082]

Another decoding person apparatus exhibits a distributed secret value, and it recovers e_0 and e_1 , it sends to the apparatus of P_j .

The apparatus of P_j checks that $E e_0 = K^{e_0} L^{e_1} \bmod p$ is formed, it stops proof, when not formed.

It is the apparatus of P_j when this is formed.

$$S_1 = w_1 + e_0 \text{ and } x_1 \bmod q$$

$$S_2 = w_2 + e_0 \text{ and } x_2 \bmod q$$

$$S_3 = w_3 + e_0 \text{ and } y_1 \bmod q$$

$$S_4 = w_4 + e_0 \text{ and } y_2 \bmod q$$

$$S_5 = w_5 + e_0 \text{ and } r \bmod q$$

$$S_6 = w_6 + e_0 \text{ and } a \bmod q$$

$$S_7 = w_7 + e_0 \text{ and } a_1 \bmod q$$

$$S_8 = w_8 + e_0 \text{ and } a_2 \bmod q$$

$$S_9 = w_9 + e_0 \text{ and } b_1 \bmod q$$

$$S_{10} = w_{10} + e_0 \text{ and } b_2 \bmod q$$

$$S_{11} = w_{11} + e_0 \text{ and } r \cdot x_1 \bmod q$$

$$S_{12} = w_{12} + e_0 \text{ and } (a \cdot x_1 + a_1) \bmod q$$

$$S_{13} = w_{13} + e_0 \text{ and } r \cdot x_2 \bmod q$$

$$S_{14} = w_{14} + e_0 \text{ and } (a \cdot x_2 + a_2) \bmod q$$

$$S_{15} = w_{15} + e_0 \text{ and } r \cdot y_1 \bmod q$$

$$S_{16} = w_{16} + e_0 \text{ and } r \cdot y_2 \bmod q$$

$$S_{17} = w_{17} + e_0 \text{ and } r \cdot y_3 \bmod q$$

$$S_{18} = w_{18} + e_0 \text{ and } r \cdot y_4 \bmod q$$

$$S_{19} = w_{19} + e_0 \text{ and } r \cdot y_5 \bmod q$$

$$S_{20} = w_{20} + e_0 \text{ and } r \cdot y_6 \bmod q$$

$$S_{21} = w_{21} + e_0 \text{ and } r \cdot y_7 \bmod q$$

$$S_{22} = w_{22} + e_0 \text{ and } r \cdot y_8 \bmod q$$

$$S_{23} = w_{23} + e_0 \text{ and } r \cdot y_9 \bmod q$$

$$S_{24} = w_{24} + e_0 \text{ and } r \cdot y_{10} \bmod q$$

$$S_{14} = w_{14} + e_0 (a \cdot x_2 + a_2) \bmod q$$

$$S_{15} = w_{15} + e_0 \cdot r \cdot y_1 \bmod q$$

$$S_{16} = w_{16} + e_0 (a \cdot y_1 + b_1) \bmod q$$

$$S_{17} = w_{17} + e_0 \cdot r \cdot y_2 \bmod q$$

$$S_{18} = w_{18} + e_0 (a \cdot y_2 + b_2) \bmod q$$

を計算して $S_1 \sim S_{18}$ および w_0 を他の復号者装置へ送付する。他の復号者装置は、

$$S_{16} = w_{16} + e_0(a \cdot y_1 + b_1) \bmod q$$

$$S_{17} = w_{17} + e_0 \text{ and } r \cdot y_2 \bmod q$$

$$S_{18} = w_{18} + e_0(a \cdot y_2 + b_2) \bmod q$$

It calculates these and sends S_1 - S_{18} and w_0 to another decoding person apparatus.

Other decoding person apparatus,

$$L = g^{w_0} \bmod p$$

$$g_1^{s_1} g_2^{s_2} = T_1 X^{e_0} \bmod p$$

$$g_1^{s_3} g_2^{s_4} = T_2 Y^{e_0} \bmod p$$

$$g^{s_5} h^{s_6} = T_3 R^{e_0} \bmod p$$

$$L = g^{w_0} \bmod p$$

$$G_1^{s_1} g_2^{s_2} = T_1 X^{e_0} \bmod p$$

$$G_1^{s_3} g_2^{s_4} = T_2 Y^{e_0} \bmod p$$

$$G^{s_5} h^{s_6} = T_3 R^{e_0} \bmod p$$

$$R^{s_1} h^{s_7} = T_4 (RX1)^{e_0} \bmod p$$

$$R^{s_2} h^{s_8} = T_5 (RX2)^{e_0} \bmod p$$

$$R^{s_3} h^{s_9} = T_6 (RY1)^{e_0} \bmod p$$

$$R^{s_4} h^{s_{10}} = T_7 (RY2)^{e_0} \bmod p$$

$$R^{s_1} h^{s_7} = T_4 (RX1)^{e_0} \bmod p$$

$$R^{s_2} h^{s_8} = T_5 (RX2)^{e_0} \bmod p$$

$$R^{s_3} h^{s_9} = T_6 (RY1)^{e_0} \bmod p$$

$$R^{s_4} h^{s_{10}} = T_7 (RY2)^{e_0} \bmod p$$

$$g^{s_{11}} h^{s_{12}} = T_8 (RX1)^{e_0} \bmod p$$

$$g^{s_{13}} h^{s_{14}} = T_9 (RX2)^{e_0} \bmod p$$

$$g^{s_{15}} h^{s_{16}} = T_{10} (RY1)^{e_0} \bmod p$$

$$g^{s_{17}} h^{s_{18}} = T_{11} (RY2)^{e_0} \bmod p$$

$$G^{s_{11}} h^{s_{12}} = T_8 (RX1)^{e_0} \bmod p$$

$$G^{s_{13}} h^{s_{14}} = T_9 (RX2)^{e_0} \bmod p$$

$$G^{s_{15}} h^{s_{16}} = T_{10} (RY1)^{e_0} \bmod p$$

$$G^{s_{17}} h^{s_{18}} = T_{11} (RY2)^{e_0} \bmod p$$

$$e^0 \bmod p$$

$$u_1^{S11+cS15} u_2^{S13+cS17} v^{-S5} = U_1^{S11+cS15} u_2^{S13+cS17} v^{-S5} = T_{12} V^{e^0 \bmod p}$$

$$T_{12} V^{e^0 \bmod p}$$

It verifies that these are formed.

が成り立つことを検証する。

【0083】

上式は、 P_j の装置が V , X , Y , R , $RX1$, $RX2$, $RY1$, $RY2$ を正しく作成した場合にのみ成り立つので、一つでも成り立たない場合は検証を失敗とする（添字 “ j ” を省略した説明は以上）。証明に失敗した復号者 P_j の装置は逸脱者であると見なされ、逸脱者の秘密値 $x1j'$, $x2j'$, $y1j'$, $y2j'$, rj を他の復号者装置が秘密値回復手順を用いて回復し、正しい V_j の値を公開する。ここでの秘密値回復手順については、例えば、文献 A.Herzberg, et.al: “Proactive secret sharing or:How to cope with perpetual leakage”, Advances in Cryptology-CRYPTO'95, LNCS 963, pp.339-352, Springer-Verlag, 1995 に詳しい。その公開された正しい V_j の値を含めて、正しい ($V1$, ..., Vn) を得る。

【0084】

($V1$, ..., Vn) の指数部が正しいことを確認した後、指数

[0083]

Since an above formula is formed only when the apparatus of P_j makes $V, X, Y, R, RX1, RX2, RY1, RY2$ correctly, when not formed at least one, it considers verification as failure (explanation which omitted the subscript “ j ” above).

It is considered that the apparatus of the decoding person P_j who failed in proof is a deviation person, another decoding person apparatus recovers a deviation person's secret value $x1j', x2j', y1j', y2j', rj$ using a secret value recovery procedure, it exhibits the correct value of V_j .

About a secret value recovery procedure here
For example, documents

It is detailed to A.Herzberg, et.al: “Proactive secret sharing or:How to cope with perpetual leakage”, Advances in Cryptology-CRYPTO'95, LNCS 963, pp.339-352, Springer-Verlag, 1995.

It includes the exhibited correct value of V_j , it obtains the correct ($V1...$, Vn).

[0084]

After the index part of ($V1...$, Vn) checks the correct thing, it decompresses a value V with

部に対する秘密復元手順により、値 V を復元する。各復号者装置は V が 1 に等しいか否かを調べ、等しくないならば復号を拒否して停止する (S 8)。等しいならば、図 4 の場合と同様に、各復号者 P_j の装置は $D_j = u \cdot 1^{z_j} \bmod p$ を計算し、放送型通信路により他の全ての復号者装置へ送信し、 D_j を受信した各復号者装置は (D_1, \dots, D_n) に対して (V_1, \dots, V_n) に対して行ったのと同様のコードワードの検証を行い、不正を検出した場合には同様に零知識証明を行って逸脱者を特定し、正しい D_j の値を秘密値回復手順を用いて回復する。

【0085】

ここでの零知識証明は以下のように実行する。 P_j の装置は乱数 d_0 を Z_q よりランダムに選択し、

$$W = g_1, \quad Q = g_1^{d_0} \bmod p$$

を他の復号者装置へ送付する。

他の復号者装置は、協力して $\text{Rand}([c_2], [c_3]) [W, Q] \rightarrow (c_{2i}, c_{3i}) (Ec_0, \dots, Ec_t)$

を実行し、 $Ec_0 = W^{c_2} Q^{c_3} \bmod p$ を P_j の装置へ送付する。

the secret decompression procedure with respect to an index part.

It examines whether each decoding person apparatus has V equal to 1, if not equal, it will refuse decoding and will stop.

(S8).

If these etc. come to be by carrying out, each decoding person's P_j apparatus will calculate $D_j = u \cdot 1^{z_j} \bmod p$ like the case of FIG. 4, it transmits to all other decoding person apparatus according to a broadcast type communication channel, each decoding person apparatus which received D_j performs verification of the coding word similar to having carried out by receiving to $(D_1, \dots, D_n) (V_1, \dots, V_n)$, when irregularity is detected, it performs zero knowledge proof similarly and specifies a deviation person, it recovers the correct value of D_j using a secret value recovery procedure.

[0085]

It performs zero knowledge proof here as follows.

The apparatus of P_j chooses a random number d_0 from Z_q at random, $w = g_1, Q = g_1^{d_0} \bmod p$

It sends these to another decoding person apparatus.

Another decoding person apparatus cooperates.

$\text{Rand}([c_2], [c_3]) [W, Q] \rightarrow (c_{2i}, c_{3i}) (Ec_0, \dots, Ec_t)$

It performs these, it sends $Ec_0 = W^{c_2} Q^{c_3} \bmod p$ to the apparatus of P_j .

【0086】

P_jの装置は乱数d₁, d₂をZ_qよりランダムに選択し、
 $T_{12} = g_1^{d_1} \bmod p$
 $T_{13} = u_1^{d_1} \bmod p$
 を計算して、他の復号者装置へ送付する。他の復号者装置は分散秘密値を公開してc₂, c₃を回復し、P_jの装置へ送付する。

【0087】

P_jの装置は $E_{c0} = W^{c_2} Q^{c_3} \bmod p$ が成り立つことを確認し、成り立たない場合は証明を中止する。これが成り立つ場合、P_jの装置は
 $S_0 = d_1 + c_2 \cdot z_1 \bmod q$
 を計算してS₀およびd₀を他の復号者装置へ送付する。他の復号者装置は、
 $Q = g_1^{d_0} \bmod p$

$g_1^{s_0} = T_{12} X_j^{c_2} \bmod p$
 $u_1^{s_0} = T_{13} D_j^{c_2} \bmod p$
 が成り立つことを検証する。

【0088】

上式は、P_jの装置がD_jを正しく作成した場合にのみ成り立つので、一つでも成り立たない場合は検証を失敗とする。各復号者装置は、正しい(D₁, ..., D_n)から、指数部に対する秘密復元手順によって $D = u_1^z \bmod p$ を復元し、 $m = e / D$

[0086]

The apparatus of P_j chooses random numbers d₁ and d₂ from Z_q at random, $t_{12} = g_1^{d_1} \bmod p$
 $T_{13} = u_1^{d_1} \bmod p$
 It calculates these, it sends to another decoding person apparatus.
 Another decoding person apparatus exhibits a distributed secret value, and it recovers c₂ and c₃, it sends to the apparatus of P_j.

[0087]

The apparatus of P_j checks that $E_{c0} = W^{c_2} Q^{c_3} \bmod p$ is formed, it stops proof, when not formed.
 It is the apparatus of P_j when this is formed.
 $S_0 = d_1 + c_2 \text{ and } z_1 \bmod q$
 It calculates these and sends S₀ and d₀ to another decoding person apparatus.
 Other decoding person apparatus, $q = g_1^{d_0} \bmod p$

$G_1^{s_0} = T_{12} X_j^{c_2} \bmod p$
 $U_1^{s_0} = T_{13} D_j^{c_2} \bmod p$
 It verifies that these are formed.

[0088]

Since an above formula is formed only when the apparatus of P_j makes D_j correctly, when not formed at least one, it considers verification as failure.
 From the correct (D₁..., D_n), with the secret decompression procedure with respect to an index part, each decoding person apparatus decompresses $D = u_1^z \bmod p$, calculates

mod p を計算してメッセージ $m=e/D \bmod p$, and decodes Message m .
 m を復号する。

【0089】

図7に実施例2における復号者装置の機能構成例を示す。メモリ21には $x1j$, $x2j$, $y1j$, $y2j$, zj の秘密鍵が記憶され、公開値 wj , $g1$, $g2$, p , q なども記憶され、更に外部へ送信する情報、外部から受信する情報を一時記憶するためにメモリ21が用いられる。分散乱数生成部22は秘密分散器23、分散秘密検証器24、分散秘密加算器25よりなり、これらにより、秘密鍵 $x1j$, $x2j$, $y1j$, $y2j$, zj が作成され、また乱数 r の分散値 rj も生成される。ハッシュ器26により受信暗号文 E について $c=H(u1, u2)$ のハッシュ関数演算が行われ、またべき乗演算器27により $Vj = (u1^{x1j+cy1j} u2^{x2j+cy2j} v^{-1})^{rj} \bmod p$ の演算が行われる。秘密分散部31は秘密分散器32、分散秘密検証器33よりなり、秘密値 Vj が Vjk にしきい値 $2t$ の検証可能秘密分散法により分散される。指数部秘密復元器34により、 Vk の指数部に対する秘密復元手順が実行され、BCHコードワード検証器35により $D1, \dots, Dn$ の $w1$ を底とする離散対数がBC

[0089]

The example of functional composition of the decoding person apparatus in Example 2 is shown in FIG. 7.

The secret key of $x1j, x2j, y1j, y2j, zj$ is stored in memory 21, the open values $wj, g1, g2$, and p and q etc. are also stored, furthermore, memory 21 is used in order to carry out the temporary memory of the information which it transmits to the exterior, and the information which it receives from the outside.

The distributed random-number generation part 22 is made up of the secret dispersion device 23, a distributed secret verification device 24, and a distributed secret adder 25, and secret-key $x1j, x2j, y1j, y2j, zj$ is made by these, and the distributed value rj of a random number r is also formed.

The hash function calculation of $c=H(u1, u2)$ is performed about the receiving cryptogram E with the hash device 26, moreover, it is $Vj=$ (the calculation of $u1^{x1j+cy1j} u2^{x2j+cy2j} v^{-1})^{rj} \bmod p$ is performed.) by the power calculator 27.

The secret dispersion part 31 is made up of a secret dispersion device 32 and a distributed secret verification device 33, and the secret value Vj is dispersed by Vjk with a threshold value of $2t$ verifiable secret dispersion method.

With the index part secret decompression device 34, the secret decompression procedure with respect to the index part of Vk is performed, and it is checked that the discrete

H符号のコードワードであることが確認される。放送型通信受信器36、放送型通信送信器37、個別通信受信器38、個別通信送信器39が設けられ、更に制御部41により各部が順次動作させられる。

【0090】

図8に実施例3に用いられる復号者装置の機能構成を、図7と対応する部分に同一番号を付けて示す。分散乗算手段43により、乱数 r と秘密鍵 x_1 の積をしきい値 t の秘密分散法により分散した値 x_{1j}' 、同様な値 x_{2j}' , y_{1j}' , y_{2j}' が求められる。証明部44は乱数生成器45、べき乗演算器46、乗余乗算・加算器47よりなり、 V_j が $u_1^{x_{1j}'+cy_{1j}'}u_2^{x_{2j}'+cy_{2j}'}v^{-r_j} \bmod p$ の計算結果であることを零知識証明によって他の復号者に証明する。零知識証明手順中の検証は検証部48のべき乗演算器49と比較器51により行われる。

【0091】

【発明の効果】

Cramer-Shoup 暗号における復

logarithm which uses w_1 of $D_1...D_n$ as a bottom with the BCH coding word verification device 35 is the coding word of a BCH code.

The broadcast type communication receiver 36, the broadcast type communication transmitter 37, the individual communication receiver 38, and the individual communication transmitter 39 are provided, furthermore, the control part 41 lets each part carry out a sequential operation.

[0090]

The same number is numbered and shown in the part which corresponds the functional composition of the decoding person apparatus used for FIG. 8 at Example 3 with FIG. 7.

By the distributed multiplication means 43, value x_{1j}' which dispersed the product of a random number r and a secret key x_1 with the secret dispersion method of threshold-value t , similar value x_{2j}' , y_{1j}' , and y_{2j}' are called for.

Proof part 44

Random-number generation device 45, power calculator 46, a remainder multiplication and adder 47

It is made up of these, it proves that V_j is the calculation result of $u_1^{x_{1j}'+cy_{1j}'}u_2^{x_{2j}'+cy_{2j}'}v^{-r_j} \bmod p$ to another decoding person by zero knowledge proof.

Verification in zero knowledge proof procedure is performed by the power calculator 49 and comparator 51 of the verification part 48.

[0091]

[ADVANTAGE OF THE INVENTION]

Since the correctness of a cryptogram is

号時の検証式の値を、この発明では復号者の誰もがその値を知り得ない乱数によってべき乗した値が1となるか否かを検証することによって暗号文の正当性を検証しているため、べき乗した値を公開しても、本来の検証式における値に関する情報は一切漏洩しない。この値が正しく作成されたことを零知識証明によって第三者へ証明する事により、受信した暗号文が元の検証式を満足しないことを第三者へ証明することができる。

【0092】

さらに、乱数でべき乗するという計算を分散計算により、全計算者の協力で行うことによって、検証式を満たさない場合にも、べき乗する前の検証式の値がどの復号者にも漏洩することはないため、復号者の中に不正者がいたとしても、攻撃者は何の利益も得ることができないため、選択的暗号文攻撃に対して安全なしきい値付き復号方法となっている。

【0093】

更にこの発明の別の観点によれば、零知識証明によって計算結果の正当性を各復号者に証明させることによって不正者を特定し、正当なデータのみを用いて暗号文の検証を行うため、復号

verified by verifying whether the value which carried out the power of the value of the verification type at the time of decoding in a Cramer-Shoup code with the random number with which everyone of a decoding person cannot know that value in this invention is set to 1, even if it exhibits the value which carried out the power, it reveals no information about the value in an original verification type.

By proving to a third person that this value was made correctly by zero knowledge proof, it can prove to a third person that the cryptogram which received does not satisfy the original verification type.

[0092]

Since the value of the verification type before carrying out a power is not revealed to all the decoding person, either, also when not filling a verification type by furthermore performing calculation of carrying out a power by random numbers, by cooperation of all accountants by distributed calculation, even if there is an irregular person in a decoding person, since an aggressor can get no profits, he is the decoding method with a safe threshold value to the alternative cryptogram attack.

[0093]

Furthermore, according to another viewpoint of this invention, it specifies an irregular person by letting each decoding person prove the correctness of a calculation result by zero knowledge proof, since verification of a cryptogram is performed only using rightful

者の数 n に比例した計算量で検証を行うことが可能である。また、各復号者の計算結果が BCH 符号のコードワードとなるように各復号者の固有の公開値を定め、まず、計算結果がコードワードであることを受信者が検証し、コードワードでない場合にのみ零知識証明を実行することによって、正しい暗号文を受信した場合には、通信量を抑えたまま効率的な計算を行うことが可能である。

【0094】

さらに、不正者が特定された場合に、他の復号者が協力してその不正な復号者が持つ分散秘密鍵を算出し、公開することによって、だれもがその不正な復号者に代わって正しい結果を計算することができるようにすることによって、 $1/3$ 以上の不正者が存在しても、それが $1/2$ 未満である限りにおいて、正しい検証結果および復号結果を得ることが可能である。

【図面の簡単な説明】**【図 1】**

この発明の実施例 1 のシステム構成を表す図。

【図 2】

data, it can perform verification by the computational complexity proportional to several n of a decoding person.

Moreover, it sets each decoding person's inherent open value that each decoding person's calculation result constitutes the coding word of a BCH code, and a receiving party verifies first that a calculation result is the coding word, when the correct cryptogram is received by performing zero knowledge proof only when it is not the coding word, it can perform efficient calculation, with the amount of communication restrained.

[0094]

Furthermore, another decoding person computes the distributed secret key which the irregular decoding person has in cooperation with the case where an irregular person is specified, although it also becomes bored by opening to the public, even if the irregular person more than $1/3$ exists by enabling it to calculate the correct result instead of the irregular decoding person, as long as it is under $1/2$, it can obtain the correct verification result and a decoding result.

[BRIEF DESCRIPTION OF THE DRAWINGS]**[FIG. 1]**

The figure showing the system assembly of Example 1 of this invention.

[FIG. 2]

この発明の実施例 1 における復号者装置の検証動作手順を示す流れ図。

The flowchart showing the verification action procedure of the decoding person apparatus in Example 1 of this invention.

【図 3】

この発明の実施例 2 のシステム構成を表す図。

[FIG. 3]

The figure showing the system assembly of Example 2 of this invention.

【図 4】

この発明の実施例 2 における復号者 P_i の装置の復号動作手順を示す流れ図。

[FIG. 4]

The flowchart showing the decoding action procedure of the decoding person's P_i apparatus in Example 2 of this invention.

【図 5】

この発明の実施例 2 における復号者 P_i の装置の検証動作手順を示す流れ図。

[FIG. 5]

The flowchart showing the verification action procedure of the decoding person's P_i apparatus in Example 2 of this invention.

【図 6】

この発明の実施例 3 における復号者 P_i の装置の検証動作手順を示す流れ図。

[FIG. 6]

The flowchart showing the verification action procedure of the decoding person's P_i apparatus in Example 3 of this invention.

【図 7】

実施例 2 における復号者装置の機能構成を示す図。

[FIG. 7]

The figure showing the functional composition of the decoding person apparatus in Example 2.

【図 8】

実施例 3 における復号者装置の機能構成を示す図。

[FIG. 8]

The figure showing the functional composition of the decoding person apparatus in Example 3.

【図 1】

[FIG. 1]

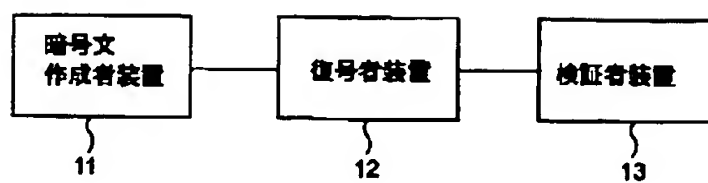


図 1

FIG. 1

11 Cryptogram maker apparatus

12 Decoding person apparatus

13 Verification person apparatus

【図 2】

[FIG. 2]

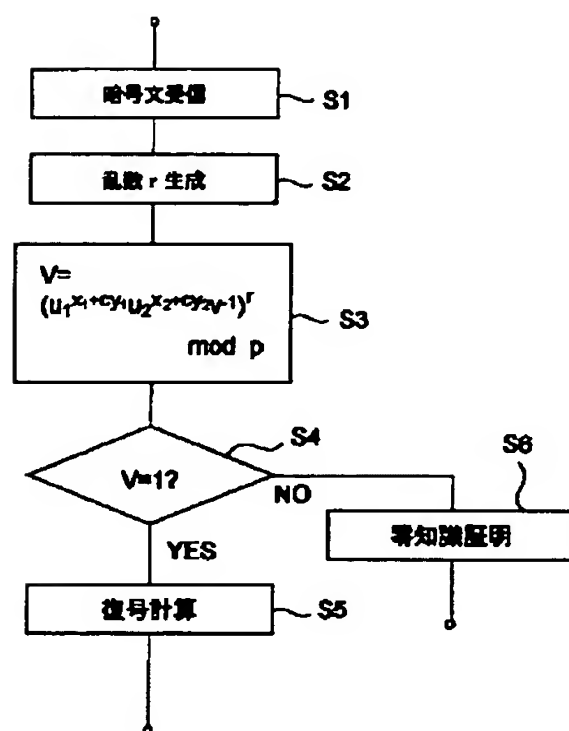


図 2

FIG. 2

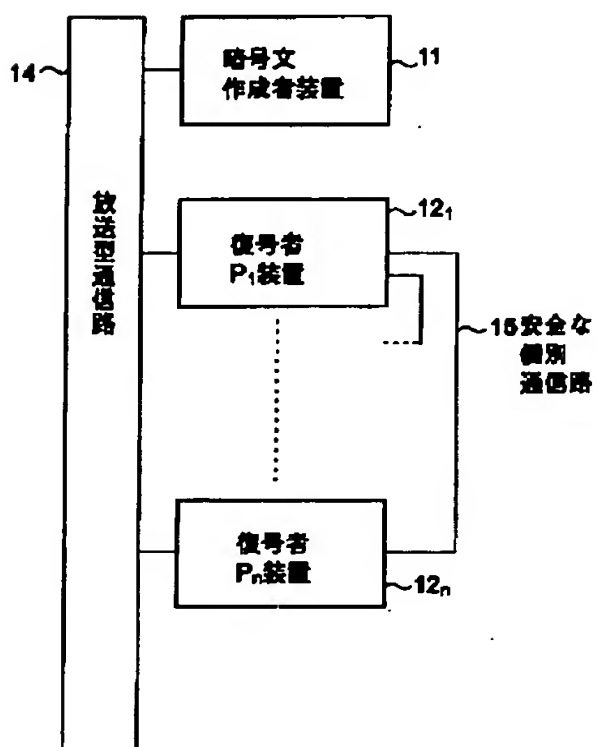
S1 Cryptogram reception

S2 Random-number r generation

S5 Decoding calculation
S6 Zero knowledge proof

【図 3】

[FIG. 3]



3

FIG. 3

- | | |
|-----|---------------------------------------|
| 11 | Cryptogram maker apparatus |
| 121 | Decoding person P1 apparatus |
| 12n | Decoding person Pn apparatus |
| 14 | Broadcast type communication channel |
| 15 | Safe individual communication channel |

【図 4】

[FIG. 4]

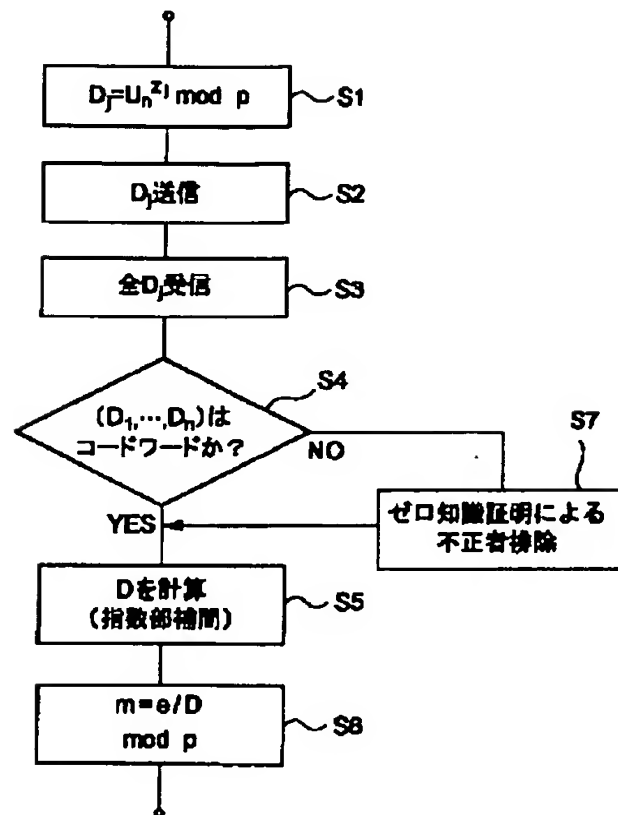


図 4

FIG. 4

S2 D_j transmissionS3 All D_j receptionS4 Are (D_1, \dots, D_n) coding words?S5 It calculates D (index part interpolation).

S7 Irregular person rejection by zero knowledge proof

【図 5】

[FIG. 5]

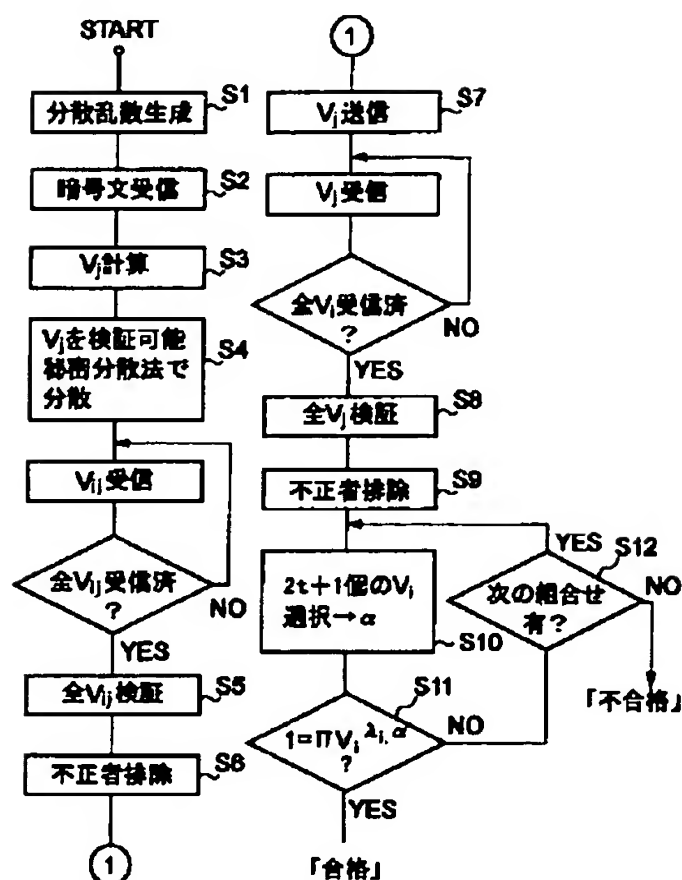


図 5

FIG. 5

START

S1 Distributed random-number generation

S2 Cryptogram reception

S3 Vj calculation

S4 It disperses Vj with verifiable secret dispersion method.

Vij reception

All Vij received ?

S5 All Vij verification

S6 Irregular person rejection

S7 Vj transmission

Vj reception

All Vj received ?

S8 All Vj verification

S9 Irregular person rejection

S10 V_i choice of $2t+1$ piece $\rightarrow (\alpha)$

Pass

S12 The following combination Present?

↓

Failure

【図 6】

[FIG. 6]

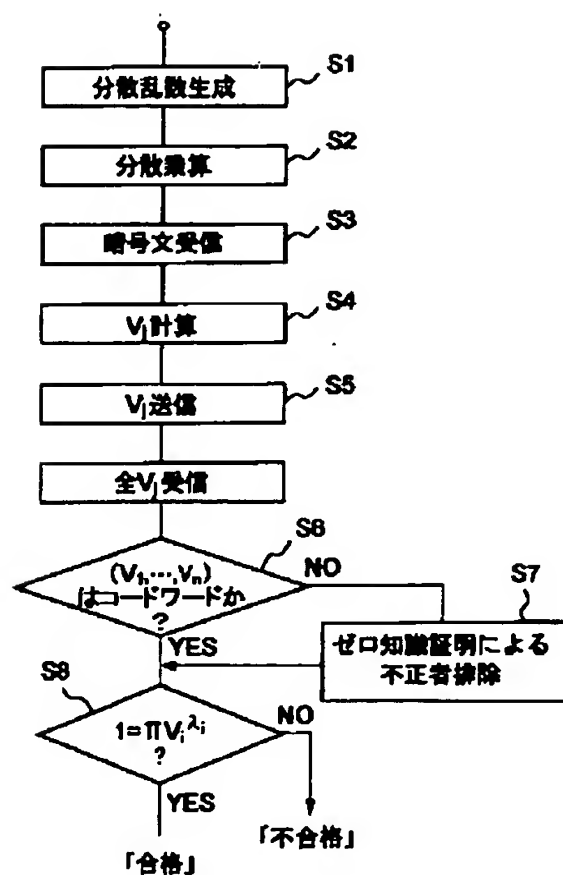


図 6

FIG. 6

S1 Distributed random-number generation

S2 Distributed multiplication

S3 Cryptogram reception

S4 V_j calculation

S5 V_j transmission

All V_j reception

S6 (V_1, \dots, V_n) Is it coding word?

S7 Irregular person rejection by zero knowledge proof

Failure

Pass

【図 7】

[FIG. 7]

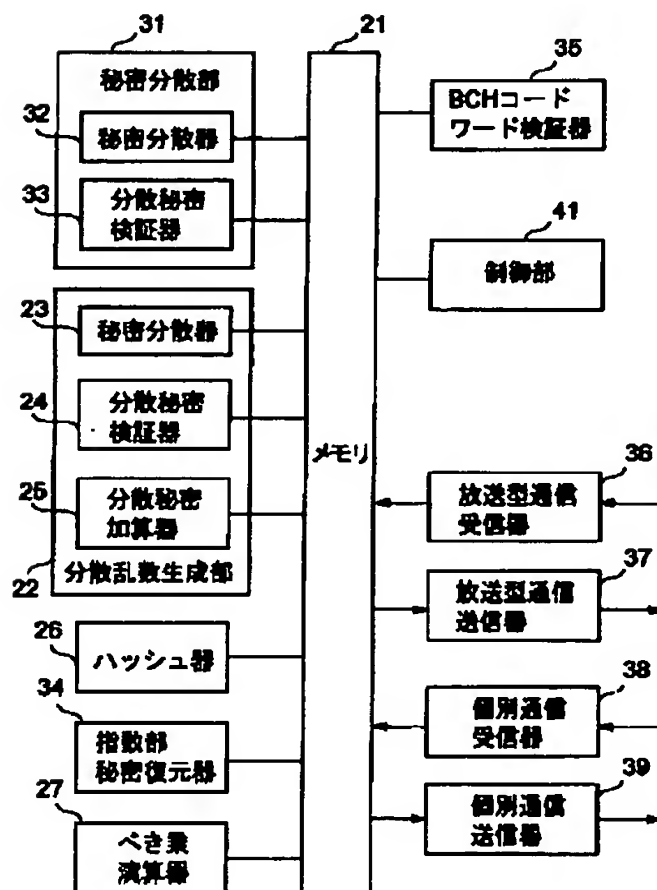


図 7

FIG. 7

- 31 Secret dispersion part
- 32 Secret dispersion device
- 33 Distributed secret verification device

- 22 Distributed random-number generation part
- 23 Secret dispersion device
- 24 Distributed secret verification device
- 25 Distributed secret adder

- 26 Hash device
- 34 Index part secret decompression device
- 27 Power calculator

- 21 Memory

- 35 BCH coding word verification device
- 41 Control part
- 36 Broadcast type communication receiver
- 37 Broadcast type communication transmitter
- 38 Individual communication receiver
- 39 Individual communication transmitter

【図 8】

[FIG. 8]

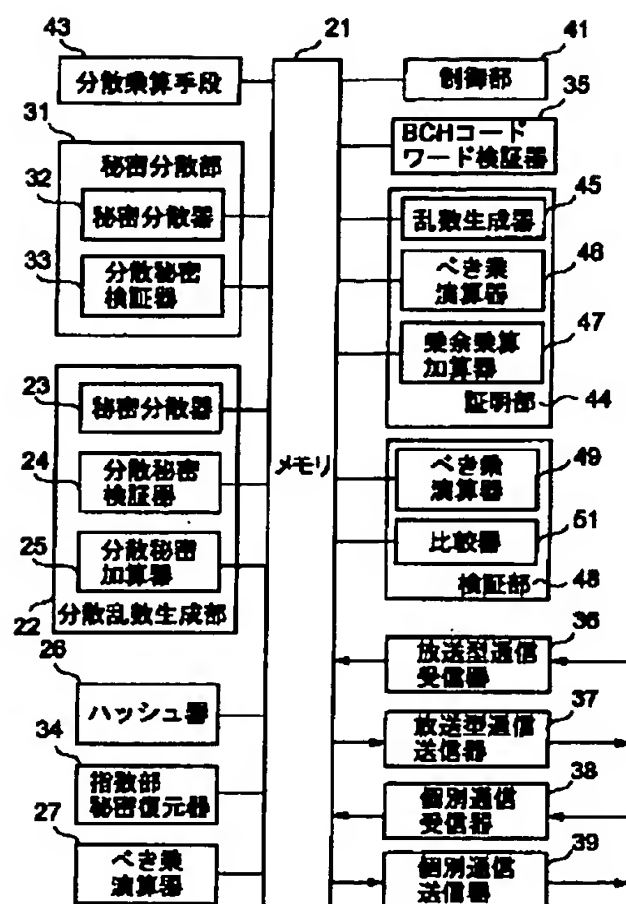


図 8

- 43 Distributed multiplication means

- 31 Secret dispersion part
- 32 Secret dispersion device
- 33 Distributed secret verification device

- 22 Distributed random-number generation part
- 23 Secret dispersion device
- 24 Distributed secret verification device
- 25 Distributed secret adder

- 26 Hash device
- 34 Index part secret decompression device
- 27 Power calculator

- 21 Memory

- 41 Control part
- 35 BCH coding word verification device

- 45 Random-number generation device
- 46 Power calculator
- 47 Remainder multiplication adder
- 44 Proof part

- 49 Power calculator
- 51 Comparator
- 48 Verification part

- 36 Broadcast type communication receiver
- 37 Broadcast type communication transmitter
- 38 Individual communication receiver
- 39 Individual communication transmitter

THOMSON SCIENTIFIC TERMS AND CONDITIONS

Thomson Scientific Ltd shall not in any circumstances be liable or responsible for the completeness or accuracy of any Thomson Scientific translation and will not be liable for any direct, indirect, consequential or economic loss or loss of profit resulting directly or indirectly from the use of any translation by any customer.

Thomson Scientific Ltd. is part of The Thomson Corporation

Please visit our website:

["www.THOMSONDERWENT.COM"](http://www.THOMSONDERWENT.COM) (English)

["www.thomsonscientific.jp"](http://www.thomsonscientific.jp) (Japanese)